TU WIEN Informatics

Ransomware-Angriffe auf Einrichtungen der kritischen Infrastruktur

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Software und Information Engineering

eingereicht von

Raphael Stamm
Matrikelnummer 00927308

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 30. Jänner 2021

Raphael Stamm	Markus Haslinger

Erklärung zur Verfassung der Arbeit

Raphael Stamm

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 30. Jänner 2021

Raphael Stamm

Kurzfassung

Aufgrund der enormen Verbreitung von digitalen Geräten in unserem täglichen Leben, gewinnt die Thematik rund um Cybersicherheit immer mehr an Bedeutung. Dies gilt vor allem im Bereich von wichtigen Industrieprozessen und Einrichtungen der kritischen Infrastruktur, wo ein Stillstand oder gar die Zerstörung von Anlagen oder Dienstleistungen weitreichende Folgen auf unser soziales und ökonomisches Leben hätte. Gerade Ransomware gilt als eine der größten Bedrohungen, wie die Angriffe der letzten Zeit gezeigt haben. Eine Ransomware ist eine Schadsoftware, die IT-Systeme sperrt oder verschlüsselt, um von den Opfern Lösegeld zu erpressen. Daher ist es das Ziel dieser Arbeit, eine Einführung in die wichtigsten und am häufigsten aufgetretenen Ransomware-Varianten zu geben. Darauf folgt eine Analyse der verheerendsten Angriffe der letzten Jahre und die dabei ausgenutzten Schwachstellen. Basierend auf dieser Analyse werden Schutz- und Gegenmaßnahmen vorgestellt, mit deren Hilfe es möglich ist, Angriffe vollständig zu verhindern oder zumindest das Schadensausmaß so gering wie möglich zu halten. Auch wird gezeigt, wie ein erfolgreich verschlüsseltes IT-System unter hoher Wahrscheinlichkeit wiederhergestellt werden kann, ohne der Lösegeldforderung in einer Kryptowährung nachzukommen. Schlussendlich gibt diese Arbeit noch einen Überblick der rechtlichen Aspekte von Ransomware-Angriffen, sowohl aus strafrechtlicher Sicht der Täter als auch der Opfer.

Abstract

Due to the enormous spread of digital devices in our daily life, the topic of cybersecurity is becoming more and more important. This is especially true in the area of important industrial processes and facilities of the critical infrastructure, where a standstill or even the destruction of plants or services would have far-reaching consequences on our social and economic life. Ransomware in particular is one of the greatest threats, as recent attacks have shown. A ransomware is a malicious software that locks or encrypts IT systems in order to extort ransom from the victims. Therefore, the aim of this thesis is to give an introduction to the most important and most common ransomware variants. This is followed by an analysis of the most devastating attacks of recent years and the vulnerabilities exploited. Based on this analysis, protective and countermeasures are presented with the help of which it is possible to completely prevent attacks or at least to keep the extent of damage as low as possible. It is also shown how a successfully encrypted IT system can be restored with high probability without paying the ransom demand in a crypto currency. Finally, this thesis gives an overview of the legal aspects of ransomware attacks, both from the perspective of the perpetrator and the victim.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES Advanced Encryption Standard

CVE Common Vulnerabilities and Exposures

ICS Industrial Control System

IoT Internet of Things

ISP Internet Service Provider

MFT Master File Table

NAS Network Attached Storage

RCE Remote Code Execution

RDP Remote Desktop Protocol

RDS Remote Desktop Services

SMB Server Message Block

StGB Strafgesetzbuch

URL Uniform Resource Locator

VBA Visual Basic for Applications

VPN Virtual Private Network

VSS Volume Shadow Copy Service

WMI Windows Management Instrumentation

KAPITEL 1

Einleitung

Die Digitalisierung unseres täglichen Lebens schreitet unweigerlich voran, von der Verwendung digitaler Geräte zur Erleichterung des Tagesablaufes, der Automatisierung von Industrieprozessen über digitale Verkehrsleitsysteme bis hin zur Telemedizin. Mit dieser enormen Verbreitung digitaler Geräte in unserem täglichen Umfeld steigt allerdings auch das Gefahrenpotential laufend an, was wie Statistiken belegen, wiederum zahlreiche Angreifer auf den Plan ruft.[1,2] Derzeit gibt es viele verschiedene Varianten von Schadsoftware wie Viren, Trojaner, Rootkits, Würmer oder Spyware.

Besonders schwerwiegend gestalten sich hierbei Angriffe auf kritische Infrastruktureinrichtungen. Dazu zählen unter anderem alle Einrichtungen oder Dienstleistungen, die bei einem Ausfall oder Zerstörung ernsthafte Konsequenzen auf unser Leben nach sich ziehen. Dabei denke man an die Versorgung mit Energie, Wasser und Nahrungsmitteln, Transportsysteme, unser Gesundheitssystem, die Finanzwelt sowie die Sicherheit durch Polizei und Militär. Fällt nur eine dieser Einrichtungen aus, kann es innerhalb kürzester Zeit verheerende Folgen wie nach einer Naturkatastrophe oder Krieg haben.

Dies zeigen die Petya / Not-Petya Ransomware-Angriffe ab März 2016 recht deutlich.[3] Ausgehend von der Ukraine wurden global zahlreiche wichtige Unternehmen von Logistik

[1] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1354.
[2] Vgl. Brewer. (2016). „Ransomware attacks: detection, prevention and cure“, S. 1.
[3] Vgl. US-CERT. (2017). „Alert (TA17-181A) Petya Ransomware“.

und Pharmaindustrie, sowie in weiterer Instanz auch Überwachungssysteme des Kernkraftwerkes in Tschernobyl lahmgelegt. Im September 2020 kam es in der Düsseldorfer Uniklinik sogar zu einem Todesfall einer Patientin, nachdem die Gesundheitseinrichtung durch die DoppelPaymer Ransomware angegriffen wurde und dadurch die sofortige Behandlung nicht möglich war und die Patientin in ein anderes Krankenhaus transportiert werden musste.[4] Daher müssen diese Einrichtungen und Dienstleistungen auch besonders gegen die in den letzten Jahren aufkommende Schadsoftware abgesichert werden.

1.1 Die erste bekannte Ransomware

Doch die weitreichenden Angriffe der letzten Zeit sind von der Art und Konzeption nicht unbedingt neu. Die erste bekannte Ransomware, der „AIDS Trojan“ oder auch „Aids Info Disk“ beziehungsweise „PC Cyborg Trojan“, geht auf das Jahr 1989 zurück.[5] Wie im Laufe der Ermittlungen des FBI bekannt wurde, verbreitete der Biologe und Harvard Absolvent Dr. Joseph Lewis Popp die erste Variante dieser Schadsoftware.[6] Als Verbreitungsweg nützte er die damals gängige Methode und duplizierte die Schadsoftware auf 5,25“ Disketten, welche dann per Post versendet wurden. Die über 22.000 Sendungen wurden auch noch mit Briefmarken frankiert, da automatische Frankiermaschinen zu dem Zeitpunkt noch eine Seltenheit waren und daher leicht zurückverfolgt werden konnten.[7]

Die Disketten enthielten neben einem Informationsprogramm zum damals noch wenig erforschten AIDS Virus, auch eine in QuickBASIC 3.0 geschriebene Datei „INSTALL.EXE“, die den eigentlichen Schadcode beinhaltete.[8] Am Ende der Installation wurde die „AUTOEXEC.BAT“ ausgetauscht und zirka nach dem 90. Neustart des angegriffenen Zielsystems wurden die Dateinamen persönlicher Nutzerdaten symmetrisch verschlüsselt und die entsprechenden Verzeichnisse vor der Benutzerin oder dem Benutzer versteckt.[9] Die Systemdateien blieben hingegen unangetastet, um es der Anwenderin oder dem Anwender zu ermöglichen, die Lösegeldforderung in Höhe von 189 USD oder 378 USD auszudrucken und per Verrechnungsscheck an ein Postfach in Panama zu begleichen.[10]

[4] Vgl. Heise. (2020). „Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau“.
[5] Vgl. Virus Bulletin. (1990). *AIDS Information Version 2.0*, S. 2.
[6] Vgl. Virus Bulletin. (1992). *Popp Goes The Weasel*, S. 2.
[7] Vgl. Virus Bulletin. (1992). *Popp Goes The Weasel*, S. 2.
[8] Vgl. Virus Bulletin. (1990). *AIDS Information Version 2.0*, S. 3.
[9] Vgl. Virus Bulletin. (1990). *AIDS Information Version 2.0*, S. 3.
[10] Vgl. Virus Bulletin. (1992). *Popp Goes The Weasel*, S. 3.

Da es sich hierbei um eine symmetrische Verschlüsselung handelte und nur die Dateinamen, nicht jedoch deren Inhalt verschlüsselt wurden, konnten Sicherheitsforscher schnell ein Werkzeug entwickeln, um die Schadsoftware rückgängig zu machen. Trotz alledem löschte ein italienisches Gesundheitsunternehmen ihre 10-jährigen Forschungsergebnisse in Panik, nachdem ein System mit dem AIDS Trojan befallen wurde.[11]

Auch die rechtliche Seite dieses Falles ist bemerkenswert, da die Schadsoftware mit dem Hinweis auf unvorhersehbare Ergebnisse ausgeliefert wurde. Die meisten Fälle traten in Großbritannien auf und dort gab es zum damaligen Zeitpunkt, abgesehen vom Computer Misuse Act 1990, noch keinerlei Gesetze, die diese Art von Cyberkriminalität unter Strafe stellten.[12]

Es sollte weitere 16 Jahre dauern, bis die Idee der Ransomware wieder aufgegriffen wurde, um im Jahre 2005 mit Hilfe der Schadsoftware GPCoder eine weltweite Angriffswelle zu starten.[13] Wie in einer Analyse des AIDS Trojan festgestellt wurde, war die größte Schwachstelle der Schadsoftware die symmetrische Verschlüsselung.[14] Durch den technologischen Fortschritt und der damit verbundenen massiv gestiegenen Rechenleistung der Systeme als auch neuer Verschlüsselungsalgorithmen, war es Angreiferinnen und Angreifern nun möglich, auch leistungsschwächere IT-Systeme anzugreifen, die oftmals zu Hause oder in Büros Verwendung finden. Die GPCoder Ransomware verwendete erstmals eine 1024 bit RSA Verschlüsselung, wodurch es zum damaligen Zeitpunkt kaum möglich war, diese zu brechen.[15] Ein weiterer Grund für die steigende Verbreitung von Ransomware ist zweifelsfrei auch die Einführung von Kryptowährungen wie Bitcoin, da hier weitgehend anonyme Transaktionen getätigt werden können.

1.2 Aufbau und Struktur

Aufgrund der mittlerweile weiten Verbreitung und dem enormen Schadpotential den Ransomware, insbesondere bei kritischen Infrastruktureinrichtungen und Dienstleistungen, anrichten kann, gibt diese Arbeit eine breite Einführung in die Thematik. Wegen der

[11] Vgl. Virus Bulletin. (1992). *Popp Goes The Weasel*, S. 2.
[12] UK Public General Acts. (1990). „Computer Misuse Act“.
[13] Vgl. Symantec. (2016). *Internet Security Threat Report*, S. 59.
[14] Vgl. Young und Moti Yung. (1996). „Cryptovirology: extortion-based security threats and countermeasures“, S. 4.
[15] Vgl. SophosLabs. (2013). *Ransomware: Next-Generation Fake Antivirus*, S. 8.

rasanten Entwicklungen in diesem Themenumfeld, werden neben wissenschaftlichen Arbeiten auch White Papers und journalistische Quellen als Literatur herangezogen.

Als Erstes werden die technischen Begriffe und Definitionen eingeführt, gefolgt von einer schrittweisen Erklärung eines Ransomware-Angriffes. Hierbei wird auch detailliert auf die Schwachstellen und Sicherheitslücken eingegangen, die zu einer Infektion führen können. Auch auf die Möglichkeiten einer Erpressung mit Hilfe der Kryptowährung Bitcoin wird hier näher eingegangen.

Gefolgt wird diese allgemeine Einführung von einigen Beispielen aktueller Ransomware-Varianten, die in letzter Zeit enormen Schaden angerichtet haben. Genauer betrachtet wird hier die zielgerichtete Ransomware Ryuk, mit deren Hilfe bisher enorme Summen an Lösegeld erpresst wurden. Weiters wird die Schadsoftware DoppelPaymer thematisiert, die für den Angriff auf die Düsseldorfer Uniklinik verwendet wurde. Aber auch auf die WannaCry sowie die verwandten Petya / Not-Petya Angriffswellen, die ausgehend von der Ukraine global enormen Schaden angerichtet haben, wird im dritten und vierten Kapitel genau eingegangen und der Ablauf eines solchen Angriffes für die Anwenderin und den Anwender illustriert.

Nach der Darstellung der Ransomware-Angriffe selbst, werden im fünften Kapitel konkrete Schutz- und Gegenmaßnahmen angeführt, mit Hilfe derer man diese Art von Angriffen komplett verhindern oder zumindest den potentiellen Schaden wesentlich verringern kann. Da die Ransomware-Varianten immer komplexer werden, benötigt man oft auch eine Vielzahl an Maßnahmen, um eine Infektion abzuwenden.

Abschließend werden noch die rechtlichen Aspekte dieser Form von Cyberkriminalität diskutiert, wobei der Schwerpunkt der Betrachtungen auf dem österreichischen Strafrecht liegt. Ergänzt wird dies durch Fallbeispiele zu zivilrechtlichen Schadensersatzansprüchen und EU-Sanktionen gegen Länder, die für staatliche Ransomware-Angriffe verantwortlich gemacht werden. Schlussendlich folgt noch ein Überblick zu bisher erpressten Lösegeldern und der aktuellen Lage.

KAPITEL 2

Ransomware

Die Anzahl an Angriffen mit Hilfe von Schadsoftware (englisch malware oder auch badware, evilware, junkware) hat in den letzten Jahren signifikant zugenommen.[16] Der Begriff umfasst alle bösartigen ausführbaren Programme, die mit voller Absicht erstellt wurden, um einer speziellen Anwendergruppe Schaden zuzufügen. Insbesondere seit dem Jahre 2006 sind wieder vermehrt Angriffe durch eine spezielle Form von Schadsoftware, der sogenannten Ransomware, zu verzeichnen.[17] Unbewusst fehlerhaft erstellte Software, die zweifelsohne auch Schaden wie beispielsweise Datenverlust hervorrufen kann, zählt allerdings nicht in diese Kategorie.

2.1 Einführung in die Schadsoftware

Schadsoftware lässt sich allgemein in folgende Arten kategorisieren:

- **Virus** (lateinisch virus, „Gift bzw. Schleim“)
  Hierbei handelt es sich um eine Schadsoftware, welche sich selbst verbreitet, sich selbst repliziert und dabei in anderen ausführbaren Programmen, in Dateien als auch in Bootsektoren oder Arbeitsspeicher (RAM) einschleust.[18] Besonderheit ist

[16] Vgl. Symantec. (2016). *Ransomware and Business, ISTR Special Report*, S. 5.
[17] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1354.
[18] Vgl. Chakraborty. (2017). „A Comparison study of Computer Virus and Detection Techniques“, S. 49.

hierbei allerdings, dass sich ein Virus nicht selbst ausführen kann und wie auch in der Natur einen Wirt (englisch host) benötigt.
Namhafte Beispiele: Michelangelo, Win32.MetaPHOR (Simile)

- **Wurm** (englisch worm)
  Im Gegensatz zum oben genannten Virus handelt es sich bei einem Wurm um eine Schadsoftware, die sich ohne einen Wirt selbstständig ausbreiten kann. Verbreitungswege sind hauptsächlich Netzwerkumgebungen und Wechseldatenträger.
  Namhafte Beispiele: Conficker, ILOVEYOU

- **Rootkit** (von englisch root, „administrativer Benutzer“)
  Ein Rootkit besteht aus einer Sammlung von Werkzeugen, mit deren Hilfe die Angreiferin oder der Angreifer versucht, auf dem zu kompromittierenden System administrativen Zugriff zu erhalten. Dabei werden bekannte Programme zur System- beziehungsweise Benutzerverwaltung manipuliert und auch Einträge aus Logdateien verändert, um die Spuren des Endringens zu verwischen.[19]
  Namhafte Beispiele: Cloaker, Vanquish, Rkit

- **Trojaner oder trojanisches Pferd** (englisch trojan horse)
  Bei einem trojanischen Pferd handelt es sich um eine Schadsoftware, welche sich als für die Benutzerinnen und Benutzer nützliche Anwendung tarnt, allerdings ohne deren Wissen im Hintergrund Schaden verursacht. Dies ist besonders schwerwiegend, da ein bereits mit dieser Schadsoftware infiziertes Gerät von selbst aus dem Inneren agieren kann.
  Namhafte Beispiele: MEMZ, FinFisher, DarkComet

- **Backdoor** (Hintertür oder englisch trapdoor)
  Um die für Benutzerinnen und Benutzer vorgesehenen Beschränkungen des Zugriffes zu umgehen, werden vorwiegend in nützlicher Software, oft auch in das Betriebssystem selbst, Hintertüren eingebaut. Dabei ist es unerheblich, ob dies vom Ersteller der Software selbst geschieht, oder beispielsweise im Nachhinein von einem Nachrichtendienst zur gezielten Quellenfernüberwachung.
  Namhaftes Beispiel: Wie in den Snowden Dokumenten im Jahre 2013 veröffentlicht,

[19] Vgl. Symantec. (2016). *Internet Security Threat Report*, S. 64.

wurde die Firmware von Produkten einiger amerikanischer Netzwerkausrüster mit einer Backdoor erweitert.[20]

- **Ransomware** (englisch ransom, „Lösegeld“)
  Erpressungssoftware, Erpressungstrojaner, Verschlüsselungstrojaner oder auch Kryptotrojaner genannt, lassen sich wiederum in drei Untergruppen einteilen.

  Während sogenannte **Locker** in erster Linie darauf abzielen den Zugang für die Benutzerinnen und Benutzer zu blockieren, verschlüsselt die **Krypto**-Variante das System selbst.[21] Dies geschieht in den meisten Fällen durch Verschlüsselung des Bootsektors (MBR), manchmal aber auch der auf dem lokalen System befindlichen persönlichen Dateien, oder des kompletten Dateisystems. Die Abgrenzung, in die eben genannten Kategorien, ist aber nicht immer zweifelfrei möglich, da es sich oft auch um Kombinationen daraus handelt. In diesem Fall spricht man von einer **Hybrid**-Ransomware, die während eines Angriffes sowohl das System für die Benutzerinnen oder Benutzer sperrt als auch gleichzeitig Dateien verschlüsselt beziehungsweise beschädigt.[22]

  Um wieder Zugang zu den verschlüsselten Dateien zu erlangen, versuchen die Angreiferinnen und Angreifer von den Benutzerinnen und Benutzern Lösegeld zu erpressen. Häufig geschieht dies in Form von einer Kryptowährung wie Bitcoin, da hierbei die Empfängerin oder der Empfänger nicht unmittelbar personalisierbar ist.[23]

  Locker Beispiele: GoldenEye, Petya, Cryptowall
  Krypto Beispiele: Cryptolocker, WannaCry, Crysis
  Hybrid Beispiele: Curve-Tor-Bitcoin (CTB) Locker, VirLock

Die Ziele als auch die Art und Durchführung dieser Ransomware-Angriffe sind sehr vielfältig. Als Geschädigte treten Privatpersonen, genauso wie Unternehmen, gemeinnützige Organisationen, Gesundheitseinrichtungen als auch Regierungen oder ganze Länder auf. Als Hauptmotiv der Kriminellen hat sich über die Jahre klar die Schädigung durch

[20] Vgl. Greenwald. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, S. 564 f.
[21] Vgl. Symantec. (2016). *Internet Security Threat Report*, S. 6.
[22] Vgl. Yaqoob et al. (2017). „The rise of ransomware and emerging security challenges in the Internet of Things“, S. 5.
[23] Vgl. Kshetri und Voas. (2017). „Do Crypto-Currencies Fuel Ransomware?“, S. 11.

einfaches Sperren des Zugriffes, die Löschung als auch die Erpressung von Lösegeld herauskristallisiert. Dies hat natürlich für die Betroffenen weitreichende Folgen, im einfachsten Fall vom Verlust der eigenen Reputation, massiver finanzieller Schaden bis hin zum Tod einer Patientin, wie der Fall an einer Düsseldorfer Uniklinik zeigt.[24] Zum Zeitpunkt der Fertigstellung dieser Arbeit hat die Staatsanwaltschaft Köln die Ermittlungen hierzu aber eingestellt.[25]

Warum gerade Ransomware-Angriffe in den letzten Jahren, nach einer unauffälligen Phase um die Jahrtausendwende, seit bekannt werden von GpCoder im Jahre 2005 wieder zunehmend an Bedeutung gewinnen, liegt in der gesteigerten Rechenleistung der Zielsysteme begründet. Außerdem bieten neuartige und effizientere Verschlüsselungsalgorithmen auch die Möglichkeit mobile Systeme als auch Internet of Things (IoT) Systeme wie Smart Homes anzugreifen.[26] In letzter Zeit ist auch zu beobachten, dass die Angreiferinnen und Angreifer die Ransomware nicht mehr selbst verwenden, sondern diese als Dienstleistung an technisch weniger versierte Kriminelle anbieten. Dabei spricht man von Ransomware as a Service (RaaS), wobei sich die GandCrab Ransomware besonders hoher Beliebtheit erfreut.[27] Einen weiteren nicht unbedeutenden Aspekt stellen in jedem Fall auch die Sozialen Medien dar, von denen sich einige Cyberkriminelle Ruhm und Bekanntheit erhoffen.

2.2 Ablauf eines Ransomware-Angriffes

Auch wenn sich die Schadsoftware selbst über die Jahre verändert und auch ausgefeilter wird, hat sich am grundsätzlichen Ablauf eines Ransomware-Angriffes wenig geändert. Dieser lässt sich wie folgt in fünf Abschnitte einteilen:[28]

- Infektion und Auslieferung (Deployment)
- Einrichtung, oftmals auch einer Backup Strategie (Installation)
- Kontrolle und Steuerung (Command-and-Control)
- Verschlüsselung oder Sperrung (Destruction)
- Benutzer Benachrichtigung und Erpressung (Extortion)

[24] Vgl. Heise. (2020). „Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau“.
[25] Vgl. Wired. (2020). „The untold story of a cyberattack, a hospital and a dying woman“.
[26] Vgl. Yaqoob et al. (2017). „The rise of ransomware and emerging security challenges in the Internet of Things“, S. 8 ff.
[27] Vgl. Bundeskriminalamt. (2019). *Cybercrime Report 2019*, S. 19.
[28] Vgl. Brewer. (2016). „Ransomware attacks: detection, prevention and cure“, S. 6.

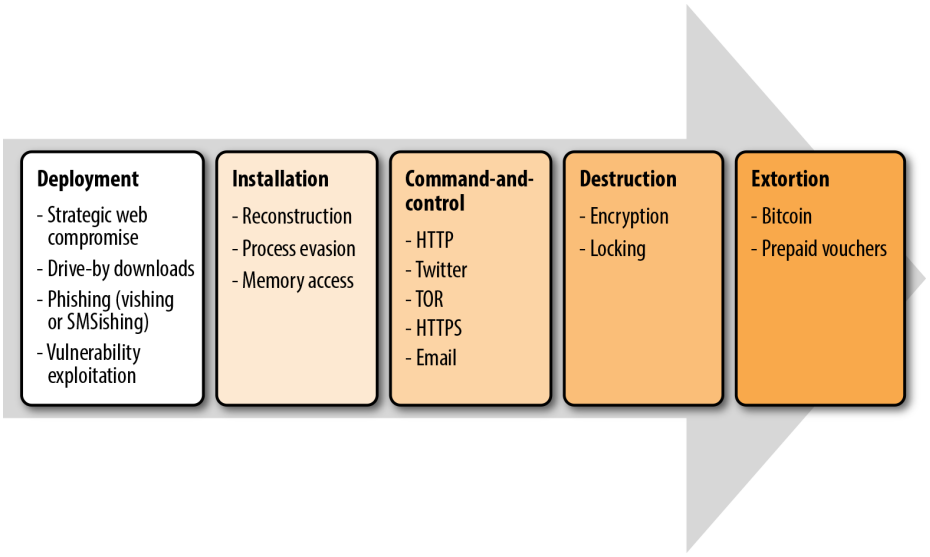

Abbildung 2.1: Allgemeiner Ablauf eines Ransomware-Angriffes[29]

Die Abbildung 2.1 zeigt den vollständigen Lebenszyklus eines Ransomware-Angriffes, welcher im folgenden Kapitel Schritt für Schritt näher beschrieben wird.

2.2.1 Infektion und Auslieferung (Deployment)

Ein Ransomware-Angriff kann sich auf ein spezielles Ziel oder eine Benutzergruppe beziehen, aber es gibt auch Varianten, die sich zufällig im Netzwerk verteilen, wenn beispielsweise auf einen Link oder Anhang in einem Phishing-E-Mail geklickt wird.

- **Drive-by downloads**
  Hierbei handelt es sich um das unbewusste Herunterladen von Schadsoftware.
- **Strategic web compromise**
  Darunter ist eine Verfeinerung von Drive-by Downloads zu verstehen, wobei gezielt Websites für eine Benutzergruppe infiziert werden. Diese Art ist wesentlich aufwendiger, da Informationen über die anzugreifenden Benutzerinnen und Benutzer vorliegen und deren häufig frequentierte Websites infiziert werden müssen.

[29] Liska und Gallo. (2016). *Ransomware: Defending Against Digital Extortion*, S. 6.

- **Software supply chain attacks**
  Als besonders gravierend erweisen sich diese Art von Angriffen, da anstatt die Opfer direkt anzugreifen, die Schwachstellen in IT-Systemen von Drittanbietern oder Zulieferern ausgenützt werden.

- **Phishing**
  Bei dieser Angriffsart werden Phishing-E-Mails mit einem Anhang oder Link auf eine infizierte Website an eine Vielzahl von potentiellen Zielen geschickt. Dies ist eine der häufigsten Verbreitungsarten und besonders effektiv bei nicht versierten Anwenderinnen und Anwendern.[30]

- **Malvertising**
  Ähnlich zu Phishing werden hierbei insbesondere harmlose Werbeeinschaltungen mit Schadcode infiziert oder Sicherheitslücken im Browser oder dessen Plug-Ins ausgenützt. Die Benutzerin oder der Benutzer muss hierbei ähnlich Drive-by Downloads nicht einmal auf einen Link klicken, um mit der Schadsoftware infiziert zu werden.

- **Vulnerability exploitation**
  Eine weitere Möglichkeit stellt die gezielte Nutzung von Schwachstellen in Systemen dar, welche durch Scannen des Netzwerkes gefunden oder einfach blind durchgetestet werden können.

2.2.2 Einrichtung (Installation)

Sobald ein Angriff auf ein Ziel gestartet wurde und der Schadcode auf das zu infizierende System heruntergeladen wurde, beginnt dieser seine Ausführung. Wie dies geschieht ist sehr von der Plattform des Zielsystems abhängig. Private Benutzerinnen und Benutzer des Windows Betriebssystems sind die am häufigsten betroffene Zielgruppe, da Windows das im Privatbereich am weitesten verbreitete Betriebssystem ist und davon ausgegangen werden kann, dass Heimbenutzerinnen und Heimbenutzer das wenigste Wissen über Schadsoftware aufweisen und daher auch in vielen Fällen keine geeignete Anti-Malware-Software besitzen.[31] Ein weiterer wichtiger Aspekt, der oftmals von dieser Zielgruppe vernachlässigt wird, ist die laufende Installation von Sicherheitsupdates. Diese

[30] Vgl. Gallegos et al. (2017). „Social engineering as an attack vector for ransomware“.
[31] Vgl. Symantec. (2016). *Ransomware and Business, ISTR Special Report*, S. 17.

und weitere wichtige Schutzmaßnahmen, werden noch detailliert im folgenden Kapitel Gegenmaßnahmen erläutert.

Da aber auch Mobilgeräte eine immer weitere Verbreitung finden, gibt es Ransomware-Angriffe auch gegen diese Plattformen.[32] Am bekanntesten für die Android Plattform ist die russische Schadsoftware Simplocker, aber auch Apples MacOS bleibt mit dem KeRanger nicht verschont. Dieser verwendet ein gefälschtes Developer Zertifikat, um die im System verankerte Überprüfung durch den Gatekeeper auszuhebeln.[33]

Eine typische Ransomware versucht als aller erstes sicherzustellen, dass sie auch nach einem Neustart ausgeführt werden kann. Hierzu wird entweder der Bootsektor infiziert oder auf Windows Systemen beispielsweise durch geeignete Schlüssel in der Registrierung. Gleichzeitig wird auch versucht die Systemwiederherstellung zu deaktivieren beziehungsweise bereits vorhandene Sicherheitskopien zu löschen oder irreparabel zu beschädigen, damit keinerlei Wiederherstellung durch die Benutzerin oder den Benutzer möglich ist.[34] Weiters werden auch Informationen über das System selbst gesammelt, indem Verzeichnisse durchsucht und ausgewertet werden.

2.2.3 Kontrolle und Steuerung (Command-and-Control)

Wenn nun eine Ransomware erfolgreich auf einem Zielsystem installiert ist, wartet sie im Normalfall auf Anweisungen von einem zentralen Kommandoserver. Hierzu baut die Schadsoftware einen sicheren Kommunikationskanal zu diesem Server auf. Um den Kommandoserver nicht rückverfolgen zu können, setzen viele Angreifer auf das Onion Routing Netzwerk TOR sowie auf dynamische Domaingeneratoren, die zufällig tausende Domains zu kontaktieren versuchen, bis ein geeigneter Server antwortet.[35] Es gibt aber auch einfache Varianten von Ransomware, die das unverschlüsselte HTTP Protokoll, den Kurznachrichtendienst Twitter oder E-Mails verwenden.

[32] Vgl. Adamov und Carlsson. (2017). „The state of ransomware. Trends and mitigation techniques“.
[33] Vgl. Symantec. (2016). *Ransomware and Business, ISTR Special Report*, S. 12.
[34] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1356.
[35] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1356.

2.2.4 Verschlüsselung oder Sperrung (Destruction)

Je nach Variante der Ransomware wird nun durch den Kommunikationskanal vom zentralen Kommandoserver ein Key für die Verschlüsselung angefordert oder lokal anhand eines eindeutigen Parameters generiert.[36] Bei einfacheren Varianten kann auch ein globaler Schlüssel verwendet werden, dies ist aber immer seltener zu beobachten. Während frühere Varianten sofort mit der Verschlüsselung der privaten Nutzerdaten begonnen haben, starten neuere Varianten zuerst mit den Volumeschattenkopien des Betriebssystems. Nachdem auch die Anti-Malware-Software immer besser und schneller solche Angriffe erkennt und zu unterbinden versucht, konzentriert sich moderne Schadsoftware zuerst auf wichtige Systemdateien oder auf die von der Benutzerin oder dem Benutzer zuletzt verwendeten Dokumente.[37]

2.2.5 Benutzerbenachrichtigung und Erpressung (Extortion)

Hat die Ransomware nun die Verschlüsselung des Systems abgeschlossen, wird das Angriffsziel mit einem Dialog darüber informiert.[38] Es werden eine Anleitung zum Bezahlen der Lösegeldsumme eingeblendet, wie auch ein Verfahren, wie das System nach Bezahlung wieder entschlüsselt werden kann. Hierbei wird aber in erster Line Angst verbreitet, um das Opfer möglichst schnell zum Bezahlen einer Lösegeldsumme zu animieren. Je nach Variante werden zur Erhöhung des Drucks auch einzelne wichtige Dateien sofort gelöscht, manchmal aber auch kostenlos entschlüsselt, um den Besitz des Entschlüsselungsparameters zu beweisen.[39] Weiterentwickelte Schadsoftware verwendet sogar vorher gesammelte Informationen des Zielsystems, um eine Lösegeldsumme festzulegen, die im finanziellen Rahmen des Opfers liegt. Bei größeren und finanzkräftigeren Unternehmen kann es sogar der Fall sein, dass die gesammelten Informationen dazu verwendet werden, um diese mehrmals zu erpressen. Generell kann daher davon nur abgeraten werden jegliche Zahlungen an die Kriminellen zu leisten, da nicht davon ausgegangen werden kann, dass diese auch den Schlüssel für die Rücksetzung des Systems in den Ausgangszustand liefern oder im schlimmsten Fall sogar weitere Erpressungsversuche unternehmen.[40]

[36] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1355.
[37] Vgl. Weckstén et al. (2016). „A novel method for recovery from Crypto Ransomware infections“, S. 1356.
[38] Vgl. Brewer. (2016). „Ransomware attacks: detection, prevention and cure“, S. 6.
[39] Vgl. Kshetri und Voas. (2017). „Do Crypto-Currencies Fuel Ransomware?“, S. 13.
[40] Vgl. Kaspersky. (2020). *Ransomware Revealed: Paying for the Protection of your Privacy*, S. 4.

Kryptowährungen (Bitcoin)

Waren in den Anfängen dieser Betrugsmasche noch aufwendige Konstruktionen mit Verrechnungsschecks und Nummernkonten in Panama notwendig, greifen die Erpresser heutzutage mit Vorliebe auf Kryptowährungen zurück.[41] Gerade die Kryptowährung Bitcoin ist hier besonders beliebt, da diese aufgrund der medialen Berichterstattung in den letzten Jahren einen hohen Bekanntheits- und Verbreitungsgrad in der Bevölkerung erreicht hat.

Bei einer Kryptowährung handelt es sich um eine digitale Komplementärwährung, die sich von einer echten Währung in einigen Punkten unterscheidet, da diese weder von einer Notenbank noch einer Regierung ausgegeben oder überwacht wird. Dies wirft natürlich auch Fragen hinsichtlich des Steuerrechtes auf und wie beispielsweise Gewinne dieser Komplementärwährung behandelt werden. Die Transaktionen, die in diesem Zahlungssystem geleistet werden, finden komplett dezentral statt, wodurch diese transparent sind und dadurch kaum gefälscht werden können.[42] Dies wird als sogenannte Blockchain bezeichnet und hat den weiteren Vorteil, dass es nicht einfach von einer Behörde oder Regierung beeinflusst oder gar gestoppt werden kann. Um die einzelnen Transaktionen zu verifizieren, errechnen die Miner einen Hashwert, der als Proof-of-Work dient.[43] Die Miner, die dafür die Rechenleistung und daher die Kosten der Transaktion tragen, werden mit Bitcoins für deren Tätigkeit entlohnt.

Internationale Transaktionen können somit problemlos in Sekundenschnelle und im Vergleich zu herkömmlichen Überweisungen äußerst kostengünstig durchgeführt werden. Mit geeigneten Verschleierungstaktiken wie der Nutzung des Onion Routing Netzwerkes TOR, können sogar anonyme Transaktionen getätigt werden. Des Weiteren ist es auch möglich Bitcoins an einen sogenannten Bitcoin-Mixer zu überweisen, welcher die Bitcoins mit denen anderer Benutzerinnen und Benutzer mischt und diese dann wieder in frei wählbaren Tranchen zurücküberweist.[44] Diese Vorgehensweise hat auch den Nachteil, oftmals von Kriminellen missbraucht zu werden.

[41] Vgl. Kshetri und Voas. (2017). „Do Crypto-Currencies Fuel Ransomware?“, S. 11.
[42] Vgl. Yuan und Wang. (2018). „Blockchain and Cryptocurrencies: Model, Techniques, and Applications“, S. 1.
[43] Vgl. Vujičić et al. (2018). „Blockchain technology, bitcoin, and Ethereum: A brief overview“, S. 2.
[44] Vgl. Bundeskriminalamt. (2019). *Cybercrime Report 2019*, S. 20.

Nachdem die Kryptowährungen keiner staatlichen Kontrolle unterliegen oder beispielsweise durch Gold gestützt werden, schwankt auch der Kurs der Komplementärwährung äußerst stark.[45] Dadurch sind diese für den Handel oder für die Bezahlung von Dienstleistungen derzeit noch kein relevanter Faktor.

[45] Vgl. Aalborg et al. (2019). „What can explain the price, volatility and trading volume of Bitcoin?“

KAPITEL 3

Beispiele der wichtigsten Ransomware-Varianten

Im folgenden Kapitel werden nun einige der wichtigsten und am häufigsten auftretenden Varianten von Ransomware vorgestellt. Besonderer Fokus liegt hierbei auf dem Angriffsvektor, also wie die Schadsoftware auf das IT-System gelangt, welchen Schaden sie dort anrichten kann und ob es gegebenenfalls Methoden zur Wiederherstellung von verschlüsselten Daten gibt.

3.1 Ryuk

Die Ryuk Ransomware erlangte erstmals im August 2018 größere Bekanntheit und gehört zu der Klasse der zielgerichteten Ransomware.[46] Hierbei handelt es sich um eine Angriffsart, wo die Cyberkriminellen gezielt ihre Opfer auswählen, um möglichst hohe Lösegeldsummen zu erpressen. Dabei kommen vor allem große finanzkräftige Unternehmen oder Einrichtungen der kritischen Infrastruktur in Frage, wo ein Ausfall oder die komplette Zerstörung des IT-Systems weitreichende Folgen hätte und daher die Bereitschaft große Summen an Lösegeld rasch zu bezahlen besonders hoch ist. Deshalb ist es den Cyberkriminellen gelungen, alleine im Zeitraum zwischen den Jahren 2018 und 2019, mehr als 61 Millionen US-Dollar zu erpressen.[47]

[46] Vgl. Malwarebytes. (2020). „Ryuk ransomware“.
[47] FBI. (2020). „Feds Fighting Ransomware: How the FBI Investigates and How You Can Help“, S. 23.

Die Ryuk Ransomware ist auch eine der ersten Schadsoftwarevarianten, der es möglich ist, gezielt im Netzwerk nach Festplatten und Geräten zu suchen und diese zu verschlüsseln. Außerdem besitzt die Schadsoftware die Fähigkeit, die Volume Shadow Copies (VSS) des Windows Betriebssystems zu löschen, damit die angegriffenen Anwenderinnen und Anwender keinerlei Möglichkeiten mehr haben, nach erfolgreicher Verschlüsselung der persönlichen Daten, diese aus der Schattenkopie wiederherzustellen.[48] Dadurch sind die Opfer gezwungen auf externe Datensicherungen zurückzugreifen.

Genau wie bei vielen anderen Ransomware-Angriffen setzen die Cyberkriminellen als Hauptangriffsvektor auf Phishing und den Versand von modifizierten SPAM E-Mails. Bei hochrangigen Angriffszielen, wie bei dieser zielgerichteten Ransomware, kommen auch Social Engineering Techniken wie Spear Phishing beziehungsweise CEO Fraud zur Anwendung. Dies wird im fünften Kapitel unter Schutz- und Gegenmaßnahmen noch im Detail erläutert. Meistens werden diese E-Mails mit Schadcode behafteten Microsoft Office Dokumenten versendet. Werden diese geöffnet, wird der Loader in der Windows PowerShell ausgeführt und weiterer Schadcode wie TrickBot nachgeladen, der wiederum Zugang zu der Ransomware Ryuk liefert.[49] Damit ist es nicht nur möglich das IT-System anzugreifen, zu verschlüsseln und Lösegeld zu erpressen, es können auch zusätzlich wichtige Zugangsdaten oder Bankdaten abgegriffen werden.

Zu den prominentesten Opfern zählen unter anderem die in den USA ansässigen Gesundheitsunternehmen Universal Health Services (UHS) und zahlreiche Nachrichtenagenturen wie The New York Times oder das Wall Street Journal.[50,51]

3.2 WannaCry / WanaDecrypt0r

Wie bereits in der Einleitung erwähnt, wurde für eine der größten bisher bekannten Ransomware-Attacken die Schadsoftware WannaCry eingesetzt. Diese infizierte bis heute mehrere hunderttausend IT-Systeme in weltweit mehr als 150 Ländern.[52] Die Kriminellen konnten bis heute nicht eindeutig identifiziert werden, aber aufgrund der Faktoren

[48] Vgl. FortiGuard Labs. (2020). „Ryuk Revisited - Analysis of Recent Ryuk Attack“, S. 4.
[49] Vgl. VMware. (2020). „VMware Carbon Black TAU: Ryuk Ransomware Technical Analysis“.
[50] Vgl. BleepingComputer. (2020). „UHS hospitals hit by reported country-wide Ryuk ransomware attack“.
[51] Vgl. Malwarebytes. (2020). „Ryuk ransomware“.
[52] Vgl. TK. (2017). „Discussion On Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks“, S. 312.

wie Komplexität und notwendiges finanzielles Budget, das für so einen Angriff aufgewendet werden muss, hat sich der Verdacht erhärtet, dass es sich um mehrere staatliche Cyberangriffe gehandelt haben muss.

Die Ransomware WannaCry wurde in der Vergangenheit auch durch folgende Namen und Begriffe bekannt:[53]

- WanaCryptor / WanaCrypt0r
- WCrypt
- WCry
- Wanna Decryptor
- WanaDecrypt0r (wahlweise mit der Versionsendung 2.0)

Wie auch im folgenden Kapitel noch genauer erläutert, verwendet die Schadsoftware WannaCry dieselbe Schwachstelle, die später auch für die Petya / Not-Petya Angriffe weltweit großflächig verwendet wurde. Hierbei handelt es sich um eine besonders schwerwiegende Schwachstelle in einem Netzwerkprotokoll (Windows SMB Protokoll der Version 1), welches vom Microsoft Windows Betriebssystem für Netzwerk-, Datei- und Druckerfreigaben verwendet wird.[54]

Besonders gravierend an dieser Schwachstelle war, dass diese aus der Ferne ausgenutzt werden konnte und die Angreiferinnen und Angreifer daher weder einen physischen Zugang auf das zu infizierende Zielsystem noch eine Interaktion der Benutzerin oder des Benutzers gebraucht haben, um weitere verwundbare IT-Systeme im selben Netzwerk zu infizieren. In diesem speziellen Fall, wenn Schadcode beziehungsweise Programme generell aus der Ferne ohne das Zutun der Anwenderin oder des Anwenders ausgeführt werden können, spricht man von Remote Code Execution. Schwachstellen die von Beginn an (Tag Null) in der Software enthalten sind und daher besonders schwerwiegend sind, werden auch als Zero-Day Exploits bezeichnet.

Die Schwachstelle im SMB Protokoll der Version 1 konnte über den TCP Port 445 ausgenützt werden, indem speziell präparierte Datenpakete an diese Schnittstelle gesendet wurden. Dies führte zu einem Pufferüberlauf (Buffer Overflow), auch Stapelüberlauf genannt, in einem Kernel Pool.[55] Hierbei werden Daten, die größer als der eigentlich

[53] Vgl. Fire Eye. (2017). „WannaCry Malware Profile“.
[54] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 1.
[55] Vgl. Check Point Research. (2017). „EternalBlue – Everything There Is To Know“.

für dieses Programm reservierte Speicherbereich sind, in den Hauptspeicher geschrieben, wodurch Speicherbereiche anderer Programme beschädigt oder manipuliert werden können. Dies führt meistens dazu, dass die in dem beschädigten Zielspeicherbereich geladenen Programme abstürzen oder diese die fälschlicherweise in den Speicherbereich geschriebenen Daten in das Programm laden.

Diese Schwachstelle wurde auch jahrelang von zahlreichen staatlichen Nachrichten- und Geheimdiensten verwendet, um Staaten mit denen das jeweilige Land in Konflikt stand auszuspionieren und gegebenenfalls wirtschaftlichen Schaden anzurichten beziehungsweise Chaos zu verbreiten.[56] Das mit weitreichenden wirtschaftlichen Sanktionen belegte Nordkorea verwendete die Lösegeldforderungen sogar dafür, ihren Devisenhaushalt aufzubessern und deren Atomwaffenprogramm zu finanzieren.[57]

Da jedoch die Hackergruppe „The Shadow Brokers“ von dieser gravierenden Schwachstelle im SMB Protokoll Erkenntnis erlangte und die Details davon stückweise im Internet veröffentlichte, sah sich der US-amerikanische Nachrichtendienst NSA dazu gezwungen, die Schwachstelle an die Firma Microsoft zu melden.[58] Dies wurde vor allem auch deshalb rasch getan, da sowohl zahlreiche eigene IT-Systeme in der US-Regierung sowie in der Wirtschaft von der Schwachstelle betroffen waren und dies zu einer massiven Bedrohung für die nationale Sicherheit werden hätte können.

Nachdem der normale Patchday ausgefallen war, veröffentlichte die Firma Microsoft am 14. März 2017 eine Aktualisierung namens MS17-01044 für die Windows SMB Server CVE-2017-0144 Remote Code Execution Vulnerability.[59] Betroffen waren die Microsoft Windows Betriebssysteme bis inklusive Windows 8.1. Aufgrund der weiten Verbreitung des Betriebssystems laufen bis zu 98 Prozent der mit WannaCry infizierten IT-Systeme unter Windows 7.[60] In der neusten Version 10 des Betriebssystems bestand die Schwachstelle jedoch nur bis zur internen Buildnummer 1511. Mit dem Creators Update hat Microsoft im Herbst 2017 schließlich das SMB Protokoll in der Version 1 bei Neuinstallationen des Windows Betriebssystems deaktiviert.[61]

[56] Vgl. The NY Times. (2017). „Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core“.
[57] Vgl. BBC. (2019). „North Korea stole 2bn USD for weapons via cyber-attacks“.
[58] Vgl. SophosLabs. (2019). *WannaCry Aftershock*, S. 3.
[59] Vgl. Microsoft Security Bulletin. (2017). „MS17-010 - Critical“.
[60] Vgl. SophosLabs. (2019). *WannaCry Aftershock*, S. 5.
[61] Vgl. Microsoft Tech Community. (2019). „SMB1 Product Clearinghouse“.

Die Hackergruppe „The Shadow Brokers“ veröffentlichte am 14. April 2017 folgende vier Schwachstellen:[62]

- EternalBlue
- EternalSynergy
- EternalChampion
- EternalRomance

Für die Ransomware-Angriffe mit Hilfe der WannaCry und später auch Petya / NotPetya Schadsoftware, wurde hauptsächlich von der EternalBlue Schwachstelle Gebrauch gemacht.

Ein weiterer vielfach aufgetretener Angriffsweg, der auch bei dieser Ransomware Anwendung findet, ist über gefälschte E-Mails. Dabei wird der Schadcode in einer manipulierten Datei als Anhang an ein E-Mail versendet. Bei der manipulierten Datei handelt es sich meistens um ein Microsoft Office Dokument, das ausführbare Markos enthält, die den eigentlichen Schadcode ausführen.

Um die Nutzerin oder den Nutzer zum Ausführen des Markos zu bewegen, wird auf Social Engineering Techniken wie CEO Fraud zurückgegriffen. Wie im folgenden Kapitel noch näher beschrieben wird, ist auch der WannaCry Ransomware-Angriff auf die Deutsche Bahn im Jahre 2017 auf diesen Angriffsvektor zurückzuführen.

Kurz nach dem Ausbruch der ersten WannaCry Angriffe fanden zwei britische Sicherheitsforscher, einer davon Marcus Hutchins, einen sogenannten Kill Switch für die Ransomware.[63] Die erste Version der WannaCry Schadsoftware versucht fünf verschiedene Domains zu kontaktieren, sind diese erreichbar, wird der Angriff sofort abgebrochen. Folgende Kill Switch Domains wurden von den Angreifern hierfür verwendet:[64]

- iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.test

[62] Vgl. Malwarebytes. (2016). „Petya – Taking Ransomware To The Low Level“.
[63] Vgl. SophosLabs. (2019). *WannaCry Aftershock*, S. 3.
[64] Vgl. Fire Eye. (2017). „WannaCry Malware Profile“.

Da diese Domains von den britischen Sicherheitsforschern registriert wurden, änderten die Angreifer die Domains geringfügig ab. In der neuesten Variante der WannaCry Ransomware ist dieser Kill Switch hingegen überhaupt nicht mehr zu finden.

Ist ein IT-System mit der WannaCry Ransomware erfolgreich infiziert, lädt diese automatisch weitere Malware nach und installiert ein persistentes Backdoor, um auch nach einem Neustart Zugriff auf das infizierte Zielsystem zu erhalten. Diese zusätzliche Installationssoftware namens „DoublePulsar“, die auch von dem US-amerikanischen Nachrichtendienst NSA entwickelt und von „The Shadow Brokers“ veröffentlicht wurde, wird von Microsoft mit dem Patch für die Windows SMB Server Remote Code Execution Vulnerability verhindert.[65] Zusätzlich versucht die WannaCry Ransomware sich selbst wie ein Wurm zu verbreiten, in dem sie zusätzliche Threads anlegt, die sowohl das lokale Netzwerk als auch das Internet nach der TCP Port 445 SMB Schwachstelle scannt.[66] Die folgende Abbildung 3.1 zeigt einen Dialog der Ransomware WannaCry mit einer Aufforderung zur Lösegeldzahlung.

Abbildung 3.1: WannaCry Dialog mit Aufforderung zur Lösegeldzahlung[67]

[65] Vgl. Check Point Research. (2017). „EternalBlue – Everything There Is To Know“.
[66] Vgl. Fire Eye. (2017). „WannaCry Malware Profile“.
[67] Fire Eye. (2017). „WannaCry Malware Profile“.

Danach wird ähnlich wie im folgenden Abschnitt der Petya / Not-Petya Ransomware detailliert erklärt, das infizierte Zielsystem verschlüsselt und bei Erfolg ein Dialog mit einer Lösegeldforderung in der Kryptowährung Bitcoin angezeigt. Die WannaCry Ransomware lässt allerdings in den meisten Fällen Systemordner unangetastet, um das angegriffene IT-System am Laufen zu halten und das Lösegeld einfordern zu können.[68]

In der ersten Version der Ransomware wurden hierbei 300 USD bis 600 USD von den Erpressern gefordert. Des Weiteren wird der Benutzerin oder dem Benutzer ein Counter angezeigt, um den psychischen Druck für die Opfer zu erhöhen, da wenn dieser abläuft, die Lösegeldforderung dementsprechend erhöht wird. Von den Angreifern wurden folgende Bitcoin Konten für die Erpressung verwendet:[69]

- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb9

Im folgenden Kapitel werden zahlreiche Angriffe mit Hilfe der WannaCry Ransomware im Detail vorgestellt und analysiert, sowie geeignete Schutz- und Gegenmaßnahmen vorgestellt.

3.3 EKANS / Snake

Besonders verheerend sind Ransomware-Angriffe auf Industrieanlagen oder Einrichtungen der kritischen Infrastruktur und gehören damit zu den größten Schreckensszenarien der neueren Zeit. Wie Anfang Jänner 2020 bekannt wurde, ist die EKANS Ransomware, die in der Literatur auch oftmals rückwärts geschrieben als Snake bezeichnet wird, speziell für den Angriff auf Industrieanlagen ausgelegt.[70]

Die EKANS Ransomware verfügt über eine spezielle Kill-Liste, um eine Vielzahl von industriellen Kontrollprozessen (ICS) gewaltsam zu stoppen beziehungsweise lahmzulegen.[71] Im Gegensatz zu Malware, die für den Angriff auf Industrieprozesse entwickelt wurde, kann die EKANS Ransomware hingegen nur die ICS-Prozesse stoppen, nicht aber mit diesen über eigne Befehle kommunizieren oder die Steuerung übernehmen.[72] Die

[68] Vgl. Fire Eye. (2017). „WannaCry Malware Profile“.
[69] Vgl. SophosLabs. (2019). *WannaCry Aftershock*, S. 11.
[70] Vgl. Bloomberg. (2020). „Ransomware Linked to Iran, Targets Industrial Controls“.
[71] Vgl. Dragos. (2020). „EKANS Ransomware and ICS Operations“.
[72] Vgl. Bloomberg. (2020). „Ransomware Linked to Iran, Targets Industrial Controls“.

EKANS Schadsoftware wurde in der kompilierbaren Programmiersprache Go geschrieben und verwendet eine Datei namens üpdate.exe", um ein IT-System zu infizieren.[73] Derzeit sind noch keine weitreichenden Angriffe mit Hilfe dieser Schadsoftware bekannt.

3.4 Petya / Not-Petya

Nach dem signifikanten Anstieg von Ransomware-Angriffen der letzten Jahre, vor allem durch die bekannte Locky und WannaCry Schadsoftware, trat im März 2016 erstmal eine neuartige Ransomware-Variante auf, die später unter dem Namen Petya bekannt wurde.[74,75] Diese nutzte allerdings als Angriffsvektor dieselbe Schwachstelle wie die Schadsoftware WannaCry aus, um die Rechnersysteme der Benutzerinnen und Benutzer zu befallen.[76]

Ein knappes Jahr nach dem ersten Auftreten von Petya war im Sommer 2017 eine weitere Angriffswelle zu verzeichnen. Wie sich allerdings bald herausgestellt hatte, handelte es sich dabei aber um eine neuartige Variante, die eine andere Zielsetzung verfolgte als ihre ursprüngliche Version. Diese Variante, die vor allem mit der massiven Angriffswelle ab dem 27. Juni 2017 in Verbindung steht, wird in Anlehnung und gleichzeitig als Abgrenzung an die vorhergehende Variante als Not-Petya bezeichnet.[77]

Diese Unterscheidung gelang aber nicht von Anfang an, daher werden in der Literatur für die zweite Angriffswelle im Juni auch die folgenden Namen synonym verwendet:[78]

- Petya
- PetrWrap
- Petna
- Not-Petya

Alle unter diesen Namen auftretende Schadsoftware gehören ausschließlich zur Petya Ransomware-Familie. Interessant zu beobachten war, dass von der ersten Angriffswelle vom 27. Juni 2017, vor allem die Ukraine betroffen schien. Die Schadsoftware breitete sich aber aufgrund der ausgenutzten Schwachstelle schnell über ganz Europa und weiter

[73] Vgl. Dragos. (2020). „EKANS Ransomware and ICS Operations“.
[74] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 1.
[75] Vgl. Symantec. (2016). *Ransomware and Business, ISTR Special Report*, S. 5.
[76] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 1.
[77] Vgl. US-CERT. (2017). „Alert (TA17-181A) Petya Ransomware“.
[78] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 2.

in über 65 Länder der ganzen Welt aus.[79] Besonders betroffen waren neben der Ukraine auch Russland, Deutschland, Indien, Brasilien und die Vereinigten Staaten von Amerika.

Die Situation war zu diesem Zeitpunkt in vielerlei Hinsicht sehr kritisch, da neben globalen Unternehmensgiganten wie dem Werbenetzwerk WPP, der dänischen Container Schifffahrtsgesellschaft Maersk auch das Heritage Valley Health System sowie das automatische Strahlungsüberwachungssystem im Kernkraftwerk Tschernobyl betroffen waren.[80] Die Wissenschaftler vor Ort waren daher gezwungen, die Werte aus dem Überwachungssystem manuell auszulesen.

Nach Angaben der ukrainischen Cyberpolizei erfolgten die ersten Angriffe über eine Schwachstelle in der Software MeDoc, die für Retail, Fremdwährungshandel und eCommerce nach wie vor verwendet wird.[81] Dazu wurden die weltweit verfügbaren Updateserver der MeDoc Software (upd.me-doc.com.ua) manipuliert, wobei diese dann die 333KB schwere Schadsoftware an die Benutzerinnen und Benutzer ausgeliefert haben.[82] Diese an die Benutzerinnen und Benutzer ausgelieferte Schadsoftware enthielt eine mit Petya infizierte Datei namens RUNDLL32.EXE.[83] Diese Datei wurde zusätzlich noch mit gefälschten Microsoft Signaturen gezeichnet, um die Erkennung durch Anti-Malware Software zu erschweren. Durch die Infektion der Updateserver dieser Finanzsoftware ist auch die weltweite rasche Ausbreitung im Unternehmensumfeld zu erklären.

Wesentlich weitere Verbreitung fand die Schadsoftware Petya allerdings über Phishing E-Mails, welche eine ausführbare Datei oder eine Dropbox URL enthielten.[84] Je nach Verbreitungsweg unterscheiden sich die Namen der ausführbaren Dateien, den sogenannten Droppern. Auffällig ist hierbei auch, dass die ursprünglichen Symbole der ausführbaren Dateien gegen die allseits bekannten PDF und WinRAR Symbole ausgetauscht wurden, um bei den Benutzerinnen und Benutzern den Eindruck zu erwecken, es handle sich übliche Dokumente, die keinerlei Schaden anrichten können.[85]

[79] Vgl. CNBC. (2017). „Petya ransomware: All you need to know about the cyberattack and how to tell if you're at risk".

[80] Vgl. The Guardian. (2017). „Petya ransomware attack: what is it and how can it be stopped?"

[81] Vgl. The Verge. (2017). „Ukranian company that spread Petya could face criminal charges for vulnerability".

[82] Vgl. The Register. (2017). „Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide".

[83] Vgl. The Register. (2017). „Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide".

[84] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 2.

[85] Vgl. Bitdefender. (2016). *Petya Ransomware Goes Low Level*, S. 4.

Häufig verwendete Namensbezeichnungen sind:[86]

- java update checker 2.8.73.2
- jucheck.exe
- picasa 3.9.141.259
- google crash handles 1.3.29.5
- SumatraPDF Installer 3.1.1

Innerhalb des Netzwerkes wurde auch eine Schwachstelle in Microsofts SMB Protokoll ausgenutzt. Diese war besonders schwerwiegend, da die Kriminellen den Schadcode aus der Ferne ausführen konnte (Remote Code Execution), ohne dabei direkten Zugriff auf das System der Opfer zu haben. Betroffen waren vor allem die Windowsbetriebssysteme von Windows XP bis Windows 8.1, in Windows 10 allerdings nur bis zur internen Version 1511.[87]

Um möglichst viele Zielsysteme innerhalb des Netzwerkes mit sich selbst zu infizieren, setzt die Petya Schadsoftware folgende Techniken ein und sammelt Informationen über:[88]

- die IP-Adressen und dazugehöriger DHCP Server aller Netzwerkadapter
- die Clients des DHCP Servers, falls dessen Ports 445/139 geöffnet sind
- alle IP-Adressen im gleichen Subnet, definiert durch die Subnetmaske
- alle Rechner zu denen offene Verbindungen bestehen
- alle Rechner im ARP Zwischenspeicher
- alle Ressourcen im Active Directory
- alle Rechner und Server in der Netzwerkumgebung
- alle Ressourcen in der Anmeldeinformationsverwaltung, auch jene Rechner, die über die Remote Desktop Services (RDS) verbunden sind

Aufgrund der Dringlichkeit und des potentiellen Schadensausmaßes veröffentlichte Microsoft am 14. März 2017 einen Patch MS17-010[89] für die Microsoft Windows SMB Server CVE-2017-0144 Remote Code Execution Vulnerability und kurz darauffolgend am 12. Mai sogar eine Version für bis dahin nicht mehr unterstützte Betriebssysteme.[90]

[86] Vgl. Bitdefender. (2016). *Petya Ransomware Goes Low Level*, S. 4.
[87] Vgl. Microsoft Security Bulletin. (2017). „MS17-010 - Critical“.
[88] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 3.
[89] Vgl. Microsoft Security Bulletin. (2017). „MS17-010 - Critical“.
[90] Vgl. Microsoft Security Response Center. (2017). „Customer Guidance for WannaCrypt attacks“.

Dieser Programmierfehler in der SMB Implementierung wurde bis dahin auch aktiv von zahlreichen staatlichen Nachrichtendiensten, allen voran der Spezialeinheit Tailored Access Operations (T.A.O.), einer Untereinheit der amerikanischen National Security Agency (NSA), unter dem Namen EternalBlue weitreichend verwendet.[91]

Neben der Schwachstelle im SMB Protokoll, verwendet die Petya Schadsoftware auch den Fernzugriff auf die Windows Management Instrumentation (WMI). Hierbei wurde unter anderem das folgende Kommando verwendet:[92]

```
„process call create \"C:\\Windows\\System32\\rundll32.exe
 [file:///\\%22C:\Windows\perfc.dat\]
 \\\"C:\\Windows\\perfc.dat\\\" #1”
```

Sollten alle bisherigen Wege sich zu verbreiten scheitern, verwendet die Ransomware Petya laut Analysen auch das „PSEXE“, oder diesem ähnliche Toolkits.

Um die Analyse obendrein noch zusätzlich zu erschweren und die eigenen Spuren zu verwischen, führt die Schadsoftware Petya noch einige weitere Schritte zur Systembereinigung durch. Um dies zu bewerkstelligen, wird das systemeigene Logfile mit folgendem Kommando bereinigt:[93]

```
„wevtutil cl Setup & wevtutil cl System & wevtutil cl Security
 & wevtutil cl Application & fsutil usn deletejournal /D %c:”
```

Ist die Schadsoftware vollständig auf dem Zielsystem geladen, beginnt die eigentliche Hauptarbeit der Petya Ransomware, die Verschlüsselung des Systems. In welcher Weise dies geschieht, ist grundsätzlich von den vorhandenen Zugriffsrechten auf dem anzugreifenden Rechnersystem abhängig.

Hierbei unterscheidet sich die Schadsoftware Petya auch grundlegend von anderen Ransomware-Familien. Werden bei Cryptolocker und anderen Ransomware-Familien hauptsächlich die persönlichen Dateien von den Benutzerinnen und Benutzern verschlüsselt, greift die Petya Schadsoftware zu einem performanteren Ansatz.

Sind administrative Rechte auf dem anzugreifenden Zielsystem vorhanden, so werden nicht die einzelnen Dateien selbst verschlüsselt, sondern nur die Verzeichnisstruktur der

[91] Vgl. The NY Times. (2017). „Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core“.
[92] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 2.
[93] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 2.

Festplatte, die sogenannte Master File Table (MFT).[94] Damit kann das Betriebssystem nicht mehr auf die einzelnen Dateien zugreifen. Die Abbildung 3.2 zeigt einen Dialog des Betriebssystems zur Benutzerkontensteuerung, um administrative Rechte anzufordern.

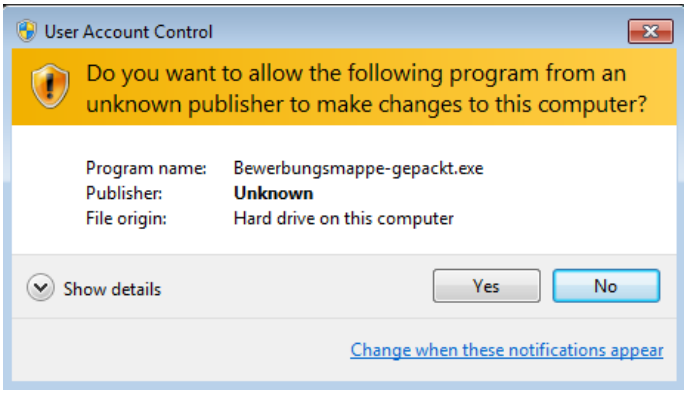

Abbildung 3.2: Dialog zur Benutzerkontensteuerung, um administrative Rechte anzufordern[95]

Um administrative Rechte zu erhalten, wird von der Schadsoftware eine Anforderung an das Betriebssystem gesendet, welches der Benutzerin oder dem Benutzer einen Dialog zur Benutzerkontensteuerung einblendet.[96] Hierbei wird auf Social Engineering zurückgegriffen, da vor allem viele technisch weniger versierte Anwenderinnen und Anwender diese Art von Dialogen einfach wegklicken, ohne weiteres Nachdenken oder den Dialog vollständig zu lesen. Hat das Betriebssystem nun der Petya Schadsoftware die nötigen administrativen Rechte gewährt, wird auch der Master Boot Record (MBR) mit einer angepassten Version überschrieben. Somit wird nach einem Neustart nicht das Betriebssystem selbst, sondern direkt die Schadsoftware geladen. Um die Benutzerin oder den Benutzer zu einem Neustart zu zwingen, wird im System ein Crash (Blue Screen of Death) verursacht.[97] Um die Benutzerin oder den Benutzer in die Irre zu führen, wird nach dem Neustart und dem Laden der Schadsoftware aus dem MBR ein gefälschter Dialog zur Windows Laufwerksüberprüfung (CHKDSK, Check Disk Scan) eingeblendet, während im Hintergrund aber die Festplatte verschlüsselt wird.[98] Die folgende Abbildung 3.3 zeigt einen gefälschten CHKDSK Dialog während der Verschlüsselung von Nutzerdaten.

[94] Vgl. Kaspersky Lab Securelist. (2017). „Schroedingers Pet(ya)“.
[95] Malwarebytes. (2016). „Petya – Taking Ransomware To The Low Level“.
[96] Vgl. Malwarebytes. (2016). „Petya – Taking Ransomware To The Low Level“.
[97] Vgl. Bitdefender. (2016). *Petya Ransomware Goes Low Level*, S. 5.
[98] Vgl. Malwarebytes. (2016). „Petya – Taking Ransomware To The Low Level“.

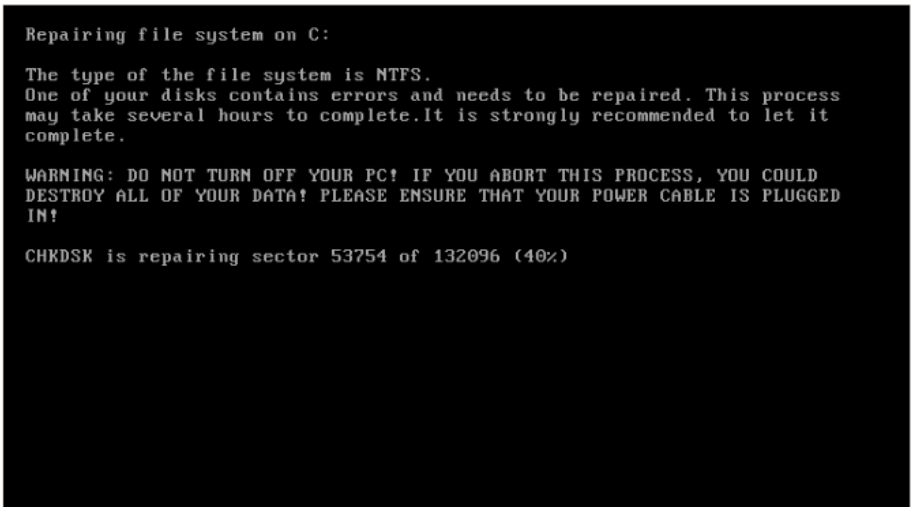

Abbildung 3.3: Der gefälschte CHKDSK Dialog während der Verschlüsselung[99]

Verfügt die Petya Ransomware hingegen nicht über genügend administrative Rechte, weil beispielsweise eine Anwenderin oder ein Anwender den Dialog zur Benutzerkontensteuerung nicht bestätigt hat, so beginnt die Schadsoftware direkt mit der Verschlüsselung der Dateien, ohne in den MBR zu schreiben oder das anzugreifende Zielsystem neu zu starten. Typischerweise werden von den Benutzerinnen und Benutzern allseits bekannte Dateitypen verschlüsselt. Die häufigsten sind hierbei:[100]

3ds,7z,accdb,ai,asp,aspx,avhd,back,bak,c,cfg,conf,cpp,cs,ctl,dbf,disk,djvu,doc,docx,
dwg,eml,fdb,gz,h,hdd,kdbx,mail,mdb,msg,nrg,ora,ost,ova,ovf,pdf,php,pmf,ppt,pptx,
pst,pvi,py,pyc,rar,rtf,sln,sql,tar,vbox,vbs,vcb,vdi,vfd,vmc,vmdk,vmsd,vmx,vsdx,vsv,
work,xls,xlsx,xvd,zip

Ein weiteres Unterscheidungsmerkmal zu bisherigen Ransomware-Varianten ist, dass bei der Petya Schadsoftware der Verschlüsselungsalgorithmus AES-128 mit RSA zum Einsatz kommt, während bei älteren Varianten Salsa20 verwendet wird.[101] Die folgende Abbildung 3.4 zeigt die verschlüsselten Dateien im Explorer, wenn keine administrativen Rechte bestehen.

[99] Malwarebytes. (2016). „Petya – Taking Ransomware To The Low Level“.
[100] McAfee Knowledge Center. (2020). „Protecting against modified Petya and BadRabbit ransomware variants“.
[101] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 2.

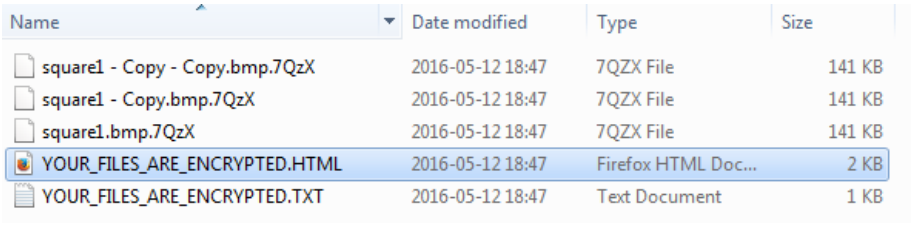

Abbildung 3.4: Verschlüsselte Dateien, wenn keine administrativen Rechte bestehen[102]

Besonders auffällig ist weiters, dass durch die Umgebung, in der die Petya Schadsoftware nach einem Neustart agiert, keine Verbindung zum Internet besteht. Somit tritt hier der ungewöhnliche Fall ein, dass die Ransomware keine Verbindung mit einem zentralen Kommandoserver herstellen kann und es dadurch unmöglich wird, von diesem Befehle zu erhalten oder Schlüssel auszutauschen.[103] Der nach der Verschlüsselung angezeigte Dialog beinhaltet nur einen zufällig generierten persönlichen Installationsparameter, der nichts mit dem tatsächlich zur Verschlüsselung verwendeten Schlüssel zu tun hat. Die folgende Abbildung 3.5 zeigt einen Dialog der Petya Ransomware nach erfolgreicher Verschlüsselung der Nutzerdaten.

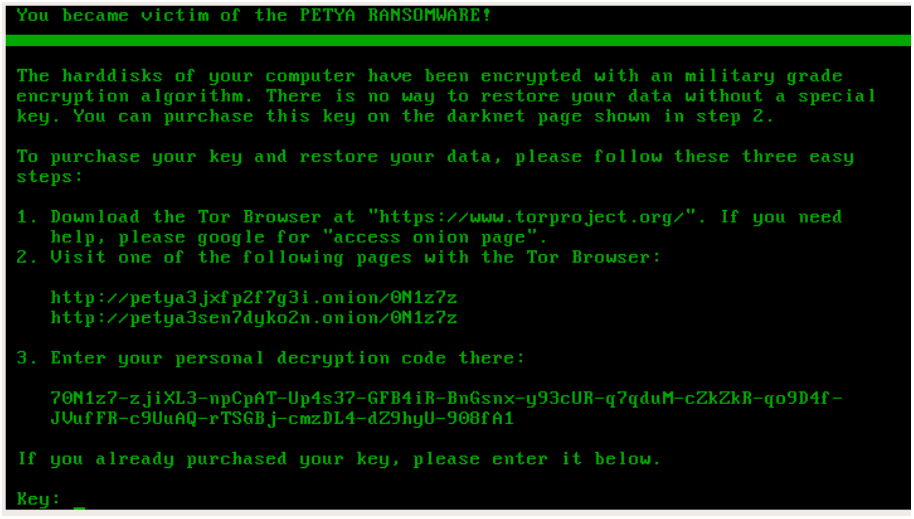

Abbildung 3.5: Petya Dialog nach erfolgreicher Verschlüsselung[104]

Auch die eingeblendete E-Mail-Adresse zur Kommunikation mit den Angreifern ist statisch und wurde umgehend vom E-Mail-Provider gesperrt. Damit ist es unmöglich, die

[102] Malwarebytes. (2017). „Bye, bye Petya! Decryptor for old versions released.“
[103] Vgl. The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack*, S. 5.
[104] Malwarebytes. (2017). „Bye, bye Petya! Decryptor for old versions released.“

verschlüsselten Dateien auf diesem Wege wiederherzustellen, aber auch für die Angreifer unmöglich an ihr Lösegeld zu kommen.[105]

Dies spricht dafür, dass es sich bei der Petya Schadsoftware eigentlich um einen Wiper handelt denn um eine echte Ransomware und das eigentliche Ziel nicht das Erpressen von Lösegeld darstellt, sondern einfach nur maximalen Schaden am anzugreifenden Zielsystem anzurichten.[106] Diese Tatsachen haben auch den Namen Not-Petya geprägt.

3.5 Bad Rabbit

Im Jahr 2017 machte noch eine andere Ransomware namens Bad Rabbit die Runde, die aber vom Schadcode her weitgehend mit Petya / ExPetr identisch ist, wobei es sich im Gegensatz zu ExPetr hierbei aber um keinen Wiper handelt und als Angriffsvektor Watering-Hole-Angriffe eingesetzt werden.[107] Hierbei handelt es sich um gezielte Angriffe, wobei speziell für eine anzugreifende Benutzergruppe häufig aufgerufene Websites mit Schadcode infiziert werden, was natürlich den Aufwand für die Cyberkriminellen erheblich erhöht. Ein bekanntes Ziel war die U-Bahn in Kiew und der Odessa Flughafen, wobei noch zusätzlich mit dem Tool Mimikatz sensible Logindaten abgegriffen wurden.[108]

[105] Vgl. Posteo. (2017). „Info on the PetrWrap/Petya ransomware: Email account in question already blocked since midday“.
[106] Vgl. Kaspersky Lab Securelist. (2017). „ExPetr/Petya/NotPetya is a Wiper, Not Ransomware“.
[107] Vgl. Kaspersky Lab Securelist. (2017). „Bad Rabbit ransomware“.
[108] Vgl. ESET. (2017). „Kiev metro hit with a new variant of the infamous Diskcoder ransomware“.

KAPITEL 4

Angriffe auf Einrichtungen der kritischen Infrastruktur

Wie schon anfangs in der allgemeinen Einführung erwähnt, stehen gerade Einrichtungen und Dienstleistungen, die zur kritischen Infrastruktur zählen, vermehrt im Fokus durch zahlreiche Hackergruppen. Dies liegt vor allem daran, dass diese kritische Infrastruktur nach einem Angriff schnell wieder in Betrieb genommen werden muss und daher die Betreiber oftmals eher bereit sind ein Lösegeld zu bezahlen, als bei weit weniger wichtigen Einrichtungen. Aus demselben Grund werden bei Angriffen auf kritische Infrastruktur weit höhere Lösegeldsummen verlangt, als bei kleineren Unternehmen oder Privatpersonen. Medizinische Universitäten und Krankenhäuser sind davon besonders stark betroffen.[109]

Dies ist unter anderem darauf zurückzuführen, dass in diesen Institutionen vielfach veraltete Systemsoftware eingesetzt wird und Sicherheitsaktualisierungen nur verspätet, wenn überhaupt, eingespielt werden. Gerade in der Zeit der COVID-19 Pandemie, in welcher grundsätzlich viel Unsicherheit herrscht, hatte dies verheerende Konsequenzen wie das folgende Fallbeispiel der Düsseldorfer Uniklinik zeigt.

[109] Vgl. Interpol. (2020). „Cybercriminals targeting critical healthcare institutions with ransomware“.

4.1 Universitätsklinikum Düsseldorf (DoppelPaymer)

Dieses wichtige deutsche Klinikum versorgt jährlich mehr als 50.000 Patientinnen und Patienten stationär sowie mehr als 300.000 ambulant. Außerdem beschäftigt es zum Zeitpunkt des Angriffes mehr als 800 Ärztinnen und Ärzte sowie über 500 Auszubildende.[110] Angreifern gelang es am 10. September 2020 etwa gegen 3 Uhr nachts das IT-System der Uniklinik weitgehend lahmzulegen.[111] Als Schadsoftware bedienten sich die Hacker der bereits vielfach verwendeten Ransomware DoppelPaymer.[112]

Diese spezielle Ransomware verschlüsselt nicht nur das anzugreifende System, sondern greift in den meisten Fällen auch noch zusätzlich Daten des Systems und der kompletten lokalen Umgebung ab. Das hat auf der einen Seite den monetären Grund, dass für die abgegriffenen Daten vielfach noch zusätzliches Lösegeld erpresst wird und anderseits, dass die Hacker darüber wertvolle Informationen gewinnen, wie ein Unternehmen oder eine kritische Infrastruktur intern aufgebaut ist. Das Wissen darüber kann nicht nur für weitere Angriffe verwendet werden, sondern auch, um die Lösegeldsumme genau an die finanziellen Möglichkeiten der Opfer anzupassen.

Um die Firewall und andere Sicherheitssysteme der Uniklinik zu umgehen, wurde eine Schwachstelle in der VPN-Software der Firma Citrix ausgenutzt. Diese als Remote Code Execution klassifizierte Schwachstelle (CVE-2019–19781), die auch als „Shitrix“ bekannt ist, wurde im vergangenen Jahr vielfach für Ransomware-Angriffe verwendet.[113] Das heimtückische an dieser Angriffswelle war, dass selbst das sofortige Einspielen von Sicherheitsupdates nicht ausgereicht hat. Das Universitätsklinikum hätte auch noch zusätzlich alle Systeme auf Schadsoftware untersuchen müssen, denn die Hacker hatten ihren Schadcode mit einer Backdoor schon im Netzwerk platziert. Damit konnten sie auch nach dem Schließen der Schwachstelle in der Citrix VPN-Software weiterhin auf das Netzwerk der Uniklinik Düsseldorf zugreifen und ihren verheerenden Angriff starten.

Der Ausfall der IT-Systeme des Uniklinikums Düsseldorf führte dazu, dass neue Patientinnen und Patienten nicht mehr aufgenommen werden konnten beziehungsweise verlegt werden mussten. Eine akut betroffene Patientin musste in ein benachbartes Wuppertaler

[110] Vgl. Universitätsklinikum Düsseldorf. (2017). „Geschäftsbericht“, S. 63.
[111] Vgl. Universitätsklinikum Düsseldorf. (2020). „IT-Ausfall an der Uniklinik Düsseldorf“.
[112] Vgl. Heise. (2020). „Uniklinik Düsseldorf: Ransomware DoppelPaymer soll hinter dem Angriff stecken“.
[113] Vgl. Citrix Systems. (2019). „CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance“.

Krankenhaus verlegt werden, wobei diese aber aufgrund der verzögerten Behandlungsmöglichkeit verstarb.[114] Die Staatsanwaltschaft Köln hat die Ermittlungen aber mittlerweile eingestellt, da die Frau in einem so schlechten Zustand war und auch ohne den Angriff verstorben wäre.[115]

4.2 National Health Service (WannaCry)

Der National Health Service (NHS) bezeichnet das staatliche Gesundheitssystem für England und Nordirland und wurde nach dem zweiten Weltkrieg gegründet, um allen Bürgerinnen und Bürgern Zugang zur medizinischen Versorgung zu ermöglichen. Die initiale Angriffswelle der WannaCry Ransomware erfasste auch 600 Organisationen, darunter mindestens 80 Krankenhäuser und ambulante Versorgungseinrichtungen des National Health Services.[116] Hauptangriffspunkt waren die veralteten Windows XP Installationen, die verstreut über alle Organisationen nach wie vor zum Einsatz kamen und auch für kritische Behandlungssysteme verwendet wurden.[117] Daher mussten tausende kritische Operationen und Behandlungstermine abgesagt oder verschoben werden, wodurch zahlreiche Patientinnen und Patienten in andere Versorgungseinrichtungen ausweichen mussten.[118] Durch die WannaCry Angriffswelle waren allerdings nicht überdurchschnittlich mehr Todesopfer zu beklagen, der finanzielle Schaden für die zahlreichen Ausfälle wird jedoch mit mehr als sechs Millionen Euro beziffert.[119] Laut National Crime Agency wurde jedoch keinerlei Lösegeld an die Erpresser bezahlt und eine Absicherung der Firewalls durchgeführt.[120]

4.3 Kernkraftwerk Tschernobyl (Not-Petya)

Das mittlerweile stillgelegte Kernkraftwerk Tschernobyl erlangte im April 1986 weltweite Bekanntheit, als es zu dem weltweit bisher schwersten Reaktorunfall kam. Die Nuklearkatastrophe hatte globale Langzeitfolgen, die noch heute zahlreiche Kontroversen

[114] Vgl. Heise. (2020). „Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau“.
[115] Vgl. Wired. (2020). „The untold story of a cyberattack, a hospital and a dying woman“.
[116] Vgl. Ghafur et al. (2019). „A retrospective impact analysis of the WannaCry cyberattack on the NHS“, S. 1.
[117] Vgl. National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*, S. 6.
[118] Vgl. National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*, S. 8.
[119] Vgl. Ghafur et al. (2019). „A retrospective impact analysis of the WannaCry cyberattack on the NHS“, S. 2.
[120] Vgl. National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*, S. 10.

auslösen.[121] Um den zerstörten Reaktorblock sowie die Unfallstelle abzusichern, wurde mit gewaltigem Aufwand ein riesiger Sarkophag über den Ort des Geschehens gebaut. Um die radioaktive Strahlung einschätzen zu können und um Lecks im Sarkophag frühzeitig erkennen zu können, wurden auf dem Gelände zahlreiche Messstationen installiert. Gerade diese wichtigen Instrumente wurden auch von der Not-Petya Angriffswelle lahmgelegt, da diese ein betroffenes Windows Betriebssystem genutzt hatten.[122] Die Aufzeichnung der Messwerte musste, genauso wie in den zahlreich betroffenen Krankenhäusern, somit manuell mit Stift und Papier erfolgen.[123]

4.4 Verwaltung Stadtgemeinde Weiz (Netwalker)

Einen der bekanntesten Ransomware-Angriffe in Österreich hat es Mitte Mai 2020 in der steirischen Bezirkshauptstadt Weiz gegeben. Mit über 12.000 Einwohnerinnen und Einwohnern und den ansässigen internationalen Großunternehmen wie Andritz Hydro, Siemens Transformers Austria sowie dem Automobilhersteller Magna Steyr, zählt diese zu einer der bedeutendsten Industriestädte der östlichen Steiermark.[124] Die Hacker verwendeten für ihren Angriff die relativ neuartige Ransomware Netwalker, die auch unter dem Namen „Ransom.PS1.NETWALKER.B“ bekannt ist.[125]

Das besondere an der Netwalker Ransomware ist, dass es sich dabei in der neuesten Variante um eine dateilose Schadsoftware handelt. Während frühere Versionen noch als ausführbares VBScript im Umlauf waren, die auch ganze Netzwerke infizieren konnten, setzt die neuere Variante auf eine andere Strategie. Der in PowerShell geschriebene Schadcode wird direkt im Hauptspeicher ausgeführt, ohne dabei eine Binärdatei auf der Festplatte abzulegen. Dazu wird eine Technik namens Reflective Dynamic-Link Library (DLL) Injection verwendet und damit der Windows Explorer infiziert, um sich im System fest zu verankern und auch nach einem Neustart ausführbar zu bleiben.[126]

[121] Vgl. World Health Organization. (2005). „Chernobyl: the true scale of the accident“.
[122] Vgl. The Register. (2017). „Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide“.
[123] Vgl. Independent. (2017). „Petya cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack“.
[124] Vgl. Stadtgemeinde Weiz. (2020). „Stadtinformation und Geschichte“.
[125] Vgl. Trend Micro. (2020). „Threat Encyclopedia Ransom.PS1.NETWALKER.B“.
[126] Vgl. Trend Micro. (2020). „Reflective Loading Runs Netwalker Fileless Ransomware“.

Die Ransomware wird in den meisten Fällen, wie auch bei der Verwaltung der Stadtgemeinde Weiz, über Phishing-Mails verteilt. Um die Anwenderinnen und Anwender zum Öffnen des mit der Schadsoftware behafteten Anhanges zu verleiten, wird als Betreff „Informationen zum Corona Virus“ angegeben. Dies dürfte Mitarbeiterinnen oder Mitarbeiter der Stadtgemeinde dazu gebracht haben, die Netwalker Ransomware im Netzwerk der Verwaltung versehentlich auszuführen.[127] Die folgende Abbildung 4.1 zeigt einen Windows-Explorer Screenshot des Datenleaks der Stadtgemeinde Weiz.

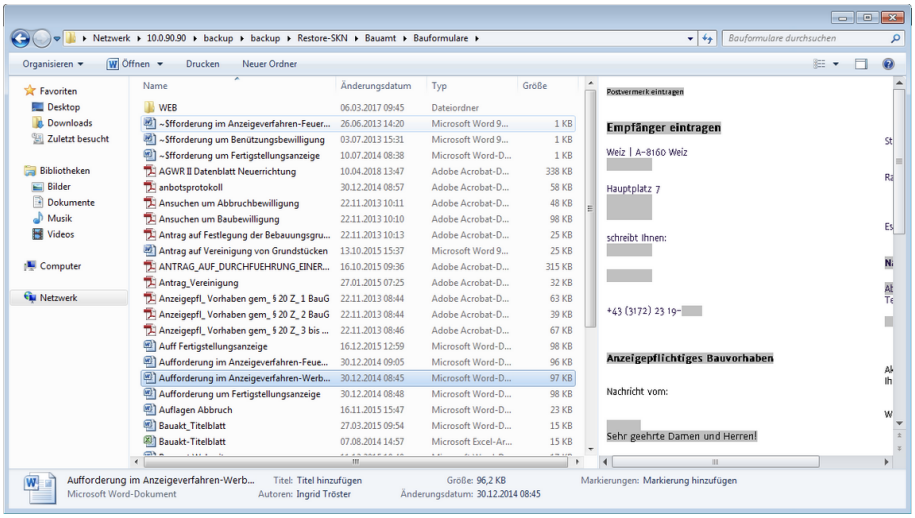

Abbildung 4.1: Screenshot des Datenleaks der Stadtgemeinde Weiz[128]

Dabei hatten die Angreifer auch Zugriff auf sensible Daten der Bürgerinnen und Bürger, wie beispielsweise aus dem Bauamt. Dies stellt auch in Hinsicht auf den Datenschutz ein enormes Problem dar, da diese persönlichen Daten wiederum für weitere Phishing-Angriffe verwendet werden können.

4.5 Deutsche Bahn (WannaCry)

Die Deutsche Bahn AG ist ein in Staatsbesitz befindliches deutsches Infrastrukturunternehmen mit mehr als 300.000 Mitarbeiterinnen und Mitarbeitern und erwirtschaftet einen jährlichen Umsatz von über 44 Milliarden Euro.[129] Im Zuge der ersten WannaCry

[127] Vgl. DerStandard. (2020). „Hacker sollen interne Daten der steirischen Stadt Weiz veröffentlicht haben“.
[128] Cyble. (2020). „NetWalker Ransomware Operators Targets City of Weiz – Data Leak“.
[129] Vgl. Deutsche Bahn AG. (2019). „Kennzahlen“.

Ransomware-Angriffswelle vom 12. bis 13. Mai 2017 wurden auch die IT-Systeme der Deutschen Bahn mit der Schadsoftware infiziert.[130] Die folgende Abbildung 4.2 zeigt eine kompromittierte Anzeigetafel der Deutschen Bahn, worauf auch der WannaCry Dialog zu sehen ist.

Abbildung 4.2: Kompromittierte Anzeigetafel der Deutschen Bahn[131]

Dabei sind auch etliche Anzeige- und Infotafeln in zahlreichen Bahnhöfen quer durch Deutschland ausgefallen.[132] Des Weiteren war auch die Infrastruktur zur Videoüberwachung von dem Ransomware-Angriff betroffen, die von der Deutschen Bahn im Auftrag der Polizeibehörden betrieben wird. Im Rahmen der WannaCry Angriffswelle sind außerdem zahlreiche Fahrkarten- und Ticketautomaten ausgefallen.[133]

[130] Vgl. Heise. (2017). „Ransomware WannaCry befällt Rechner der Deutschen Bahn“.
[131] The Telegraph. (2017). „Cyber attack hits German train stations as hackers target Deutsche Bahn“.
[132] Vgl. The Telegraph. (2017). „Cyber attack hits German train stations as hackers target Deutsche Bahn“.
[133] Vgl. Heise. (2017). „Ransomware WannaCry befällt Rechner der Deutschen Bahn“.

KAPITEL 5

Schutz- und Gegenmaßnahmen

Im folgenden Kapitel werden nun Strategien und Maßnahmen vorgestellt, um den Angriff mit Hilfe einer Ransomware zu erkennen, einzuordnen und im besten Fall das System so zu schützen, um gar nicht erfolgreiches Ziel eines Angriffes zu werden. Da die Methoden und Varianten der Schadsoftware über die Jahre immer ausgefeilter und aufwendiger wurden, ist es nicht ausreichend nur eine einzelne Maßnahme umzusetzen, sondern es bedarf einer Vielzahl von Gegenmaßnahmen. Des Weiteren wird auch aufgezeigt, welche Schritte unternommen werden sollten, falls es doch zu einer erfolgreichen Ransomware-Infektion kommen sollte und wie die verschlüsselten Daten wiederhergestellt werden können, ohne die Angreifer zu kontaktieren oder ein Lösegeld zu bezahlen.

5.1 Erkennung eines Ransomware-Angriffes

Je früher ein Ransomware-Angriff erkannt wird, desto besser stehen die Chancen den verursachten Schaden in Grenzen zu halten beziehungsweise überhaupt abzuwenden. Hierzu bieten sich vor allem für größere Unternehmen und Organisationen Intrusion Detection Systeme an, die den Netzwerkverkehr anhand von Signaturen laufend überwachen. Diese erkennen außerdem Anomalien, die lokale Systeme aufgrund des beschränkten Informationsstandes oftmals nicht analysieren können.[134]

[134] Vgl. Brewer. (2016). „Ransomware attacks: detection, prevention and cure“, S. 8.

Aber auch für kleinere Unternehmen oder Privatnutzerinnen und Privatnutzer gibt es Möglichkeiten Ransomware-Angriffe frühzeitig zu erkennen. Einige Ransomware-Varianten versuchen nämlich als erstes das System und die lokale Netzwerkumgebung auszuspionieren beziehungsweise mit entsprechenden Loadern weitere Schadsoftware nachzuladen, bevor der eigentliche Verschlüsselungsvorgang eingeleitet wird. Somit ist es unter Umständen auch für Laien möglich einen Angriff zu erkennen, wenn beispielsweise der eigene Rechner bei Nichtverwendung nicht mehr in den Ruhezustand übergeht oder die Aktivitätsanzeige durchgehend aufleuchtet, obwohl kein Programm gestartet wurde.

Einige Internet Dienst Anbieter (ISP) beschränken außerdem ihr SMTP-Gateway auf einige wenige Mails pro Tag und pro Nutzerin oder Nutzer, um Missbrauch durch SPAM oder Massenwerbung zu verhindern.[135] Verweigert nun das E-Mail-Programm beim Versenden seinen Dienst, kann dies ein Indiz für eine Ransomware-Infektion sein, da diese auch versucht, sich über diesen Weg zu verbreiten. Sollte es Anzeichen für eine Ransomware-Infektion geben, sollte das IT-System sofort vom Internet beziehungsweise Netzwerk getrennt werden, um eine weitere Verbreitung zu verhindern oder gleich das ganze IT-System heruntergefahren werden, um weiteren Schaden der eigenen Daten abzuwenden.

5.2 Einordnung eines Ransomware-Angriffes

Aufgrund der Vielzahl an Ransomware-Varianten, die laufend veröffentlicht werden, ist es besonders schwierig diese korrekt einzuordnen und entsprechende Gegenmaßnahmen einzuleiten. Zusätzlich erschweren Mutationen die Erkennung. Das sind Schadsoftware-Varianten, die zwar als Basis eine bekannte Ransomware nutzen, aber geringfügig verändert werden oder mit zusätzlichen Mechanismen gebündelt werden, um vorhandene Analysewerkzeuge zu umgehen.

Eingeordnet wird die Ransomware allgemein in die im zweiten Kapitel eingeführten Klassen Locker, Krypto und Hybrid. Eine weitere Klassifikation wäre auch nach den Eigenschaften verschlüsselnder und nicht-verschlüsselnder Ransomware möglich, beziehungsweise ob es sich um einen gezielten Angriff (targeted Ransomware) handelt.

[135] Vgl. Internet Engineering Task Force. (1999). „Anti-Spam Recommendations for SMTP MTAs“.

5.3 Wiederherstellung im Falle eines erfolgreichen Ransomware-Angriffes

Wurde die lokale Festplatte oder auch nur einzelne persönliche Daten der Anwenderin oder des Anwenders verschlüsselt, gibt es zwei Wege um das System zu säubern und auf den Stand vor dem Angriff wiederherzustellen.

5.3.1 Zurücksetzen des Systems und Wiederherstellen

Die erfolgversprechendste Lösung ist die komplette Löschung des Systems beziehungsweise das Zurücksetzen des Gerätes in den Werkszustand und anschließend die Wiederherstellung der persönlichen Dateien aus einem vor dem Angriff erstellten Backup.

5.3.2 Entschlüsselung des Systems und Entfernung der Schadsoftware

Sind die Hintergründe des Angriffes bekannt, insbesondere welche Ransomware genau verwendet wurde und welche Sicherheitslücken im System ausgenutzt wurden, kann man auch den folgenden Ansatz wählen. Zuerst wird das System in einem Safe Mode gestartet, um den Dialog zur Lösegeldforderung zu umgehen und dann wird mit Hilfe einer Anti-Malware-Software die Ransomware komplett vom System entfernt. War dieser Vorgang erfolgreich, wird die Festplatte selbst anhand von geeigneten Werkzeugen entschlüsselt.

Als Allererstes muss also die Schadsoftware selbst entfernt werden. Dies ist besonders wichtig, da diese sich sonst immer wieder selbst neu ausführen und das infizierte IT-System abermals verschlüsseln kann. Dazu ist es bei IT-Systemen notwendig, auf denen ein Windows Betriebssystem installiert ist, diese im sogenannten abgesicherten Modus neu zu starten. Dazu muss auf allen gängigen IT-Systemen während des Startvorganges die F8 Taste mehrmals gedrückt werden, bis ein entsprechendes Fenster mit erweiterten Startoptionen angezeigt wird. Hierbei gibt es zwei Möglichkeiten, den abgesicherten Modus nur mit der Befehlseingabe oder zusätzlich noch mit Netzwerkfunktionalität zu starten. Die Netzwerkfunktionalität erleichtert das Nachladen einer Anti-Malware-Software, diese kann jedoch in seltenen Fällen von der Ransomware unterbrochen werden, dann sind zusätzliche Schritte notwendig.

Da es mittlerweile hunderte verschiedene Varianten von Ransomware gibt, eignet sich ein Tool wie „Crypto Sheriff“ um herauszufinden, mit welcher Schadsoftware das eigene

System genau infiziert wurde.[136] Ist die Art der Ransomware bekannt, kann auch gleich ein entsprechendes Werkzeug zum Entfernen der Schadsoftware heruntergeladen und ausgeführt werden. Nach der erfolgreichen Installation und Aktualisierung der Anti-Malware-Software kann nun das komplette System auf die potentielle Infektion untersucht werden. Wurde eine Ransomware-Variante erkannt, kann diese nun vollständig vom infizierten IT-System entfernt werden.

Im nächsten Schritt muss nun das IT-System neu gestartet werden und eine entsprechende Software zur Datenwiederherstellung nachgeladen werden. Dazu gibt es mehrere Möglichkeiten, entweder die verschlüsselten Dateien durch Ausprobieren aller durch Reverse Engineering verfügbaren Schlüssel (Brute-Force) rückzusetzen oder durch Wiederherstellung der persönlichen Dateien mit Hilfe des Volume Shadow Copy Service (VSS), falls dieses vorhanden und von der Ransomware nicht gelöscht wurde.[137]

5.4 Aktuelle Strategien zur Verhinderung eines Ransomware-Angriffes

Basierend auf der Analyse der im dritten Kapitel vorgestellten Ransomware-Varianten, gibt dieser Abschnitt nun zu jedem potentiellen Angriffsvektor eine mögliche Lösung zur Prävention.

5.4.1 Laufende Sicherheitskopien

Wie im vorigen Abschnitt erwähnt, ist die regelmäßige Erstellung von Sicherheitskopien die erfolgversprechendste Lösung zur Verhinderung eines Schadens durch Ransomware. Hierbei gilt es allerdings einige Dinge zu beachten, um nicht trotzdem Opfer eines Angriffes zu werden. Die Sicherungen sollten unbedingt unabhängig vom zu sichernden System gelagert werden und nach dem erfolgreichen Sicherungsvorgang keinerlei Verbindung zu diesem mehr haben, da ansonsten einige Ransomware-Varianten auch das Backupsystem angreifen und die zuvor erstellten Sicherungskopien verschlüsseln oder gar löschen könnten.[138] Dieses Vorgehen empfiehlt sich auch aus anderen Gründen, wie beispielsweise Bränden oder Überspannungen im Stromnetz.

[136] Vgl. Europol European Cybercrime Centre. (2016). „Crypto Sheriff“.
[137] Vgl. Microsoft. (2009). „Volume shadow copy overview“.
[138] Vgl. Brewer. (2016). „Ransomware attacks: detection, prevention and cure“, S. 7.

5.4.2 Deaktivierung von Makros

Makros bieten eine Vielzahl von Möglichkeiten, um Abläufe in Microsoft Office zu automatisieren oder neue benötigte Funktionen einzuführen, die nicht im Standardumfang enthalten sind. Hierzu wird üblicherweise die von Microsoft entwickelte Skriptsprache Visual Basic for Applications (VBA) verwendet. Diese ist in allen gängigen Microsoft Office Programmen seit der Version 2000 verfügbar.[139] Die Mächtigkeit dieser Skriptsprache hat aber auch ihre Nachteile, so kann Schadcode direkt in Microsoft Office Dokumenten integriert und ausgeführt werden. Werden Makros nicht unbedingt benötigt, sollten diese daher aus Sicherheitsgründen immer deaktiviert werden. Falls dennoch Bedarf besteht, sollten die Microsoft Office Makros nur aus vertrauenswürdigen Quellen bezogen werden, dies gilt insbesondere aus dem Internet.

Um die Makros in Microsoft Office Programmen zu deaktivieren, können Endbenutzerinnen und Endbenutzer dies über das von Office zur Verfügung gestellte Trust Center bewerkstelligen. Für Unternehmen oder Organisationen mit einer großen Anzahl von Anwenderinnen und Anwendern eignet sich dieses Verfahren allerdings nicht, da technisch weniger versierte Personen diese einfach wieder aktivieren könnten. Hierzu bietet Microsoft in den Versionen für Unternehmenskundinnen und Unternehmenskunden zusätzlich die Möglichkeit die Makros zentral über Gruppenrichtlinien zu verwalten. Dazu können administrative Vorlagen erstellt werden, die dann global im ganzen Unternehmen ausgerollt werden.[140] Die Gruppenrichtlinien bieten auch die Möglichkeit interne beziehungsweise zertifizierte Makros zuzulassen, während externe aus dem Internet geladene Makros deaktiviert werden. Dies erleichtert auch die Administration erheblich, was wiederum in verbesserter Sicherheit resultiert.

5.4.3 Filterung von E-Mail-Anhängen

Um die Möglichkeiten eines Angriffes mit Hilfe einer Schadsoftware zu minimieren, sollten auch die E-Mail-Anhänge gefiltert werden und ausführbare Dateien wie beispielsweise mit der Dateiendung (.exe) blockiert werden. Diese Art von Dateien sollten entweder in komprimierter Form (.zip) oder über einen Clouddienst ausgetauscht werden.

[139] Vgl. Microsoft. (1998). „Microsoft Outlook 2000 Joins Office 2000 Suite in Supporting Visual Basic for Applications“.

[140] Vgl. Microsoft Security. (2016). „New feature in Office 2016 can block macros and help prevent infection“.

5.4.4 Deaktivierung von VBA und Windows PowerShell

Eine weitere Maßnahme zur Einschränkung von ausführbarem Schadcode wäre die komplette Deaktivierung der Skriptsprache Visual Basic for Applications (VBA). Dies ist auch über die oben genannten Gruppenrichtlinien möglich.

Die Windows PowerShell wird in neueren Versionen des Microsoft Windows Betriebssystems integriert und bietet erfahrenen Benutzerinnen und Benutzern ein mächtiges Werkzeug, um Prozesse zu automatisieren und das System zu verwalten. Diese Vielfalt an Möglichkeiten hat aber auch ihren Preis, denn sie wird von zahlreichen Ransomware-Varianten genützt, um den Schadcode auszuführen und das infizierte System zu verschlüsseln.

Die Gruppenrichtlinien bieten hierzu eine geeignete Lösung zur Einschränkung der Windows PowerShell. Hierzu werden sogenannte Ausführungsrichtlinien (Execution Policy) festgelegt, die genau regeln, ob nur lokale oder auch aus dem Internet heruntergeladene Skripte signiert sein müssen.[141] Als radikale Lösung kann die Windows PowerShell auch über das Dialogfenster „Windows-Features“ komplett deaktiviert werden.

5.4.5 Laufende Sicherheitsaktualisierungen

Der in der Ukraine ausgehende Not-Petya Ransomware-Angriff hat gezeigt, dass es auch besonders wichtig ist, das Betriebssystem, den Web-Browser und die Anti-Malware-Software immer auf dem neuesten Stand zu halten. Dadurch erhöht sich die Wahrscheinlichkeit enorm, gegen eine Vielzahl der derzeit bekannten Angriffsvektoren geschützt zu sein, weil ohne die aktuellen Signaturen neuartigere Varianten von Schadsoftware nicht erkannt werden können.

5.4.6 Zurücksetzen der Systemzeit

Moderne Ransomware-Varianten beinhalten einen Timer, um die Höhe des Lösegeldes zu steuern. Je mehr Zeit zwischen Infektion und Zahlung vergeht, desto teurer wird es für die Opfer sich freizukaufen. Sollten die ergriffenen Schutzmaßnahmen daher versagen und man doch Opfer eines Ransomware-Angriffes werden, empfiehlt sich von Zeit zu Zeit die Systemzeit (BIOS clock) zurückzusetzten, um eine Erhöhung des geforderten Lösegeldes abzuwenden.

[141] Vgl. Microsoft. (2020). „PowerShell Security Set-ExecutionPolicy“.

5.4.7 Deaktivierung von Protokollen und Diensten

Wie die Angriffe basierend auf der EternalBlue Schwachstelle in dem Windows SMB Protokoll der Version 1 gezeigt haben, stellen veraltete Netzwerkprotokolle und Systemdienste besonders gravierende Sicherheitslücken dar. Aufgrund dieser Erkenntnis sollten veraltete, nicht mehr gewartete Protokolle und Systemdienste vollständig deinstalliert oder zumindest deaktiviert werden. Dies betrifft Endanwenderinnen und Endanwender ebenso wie Administratorinnen und Administratoren in Unternehmen und Organisationen.

Gerade bei Netzwerkdruckern, Netzwerkfestplatten (NAS) oder Modem-Router Kombinationsgeräten werden standardmäßig viele Dienste aktiviert, um eine möglichst große Kompatibilität sowie eine erleichterte Einrichtung für die Anwenderinnen und Anwender zu ermöglichen. Besonderes Augenmerk sollte auch auf die neuen Smart Home sowie Internet of Things (IoT) Geräte gelegt werden, denn auch diese werden mit unzureichenden Sicherheitseinstellungen ausgeliefert, sofern diese Geräte überhaupt geeignete Schutzmaßnahmen bereitstellen können.

5.4.8 Absicherung von VPN und Remote Desktop Protocol (RDP)

Bei dem Remote Desktop Protocol (RDP) handelt es sich um ein Netzwerkprotokoll der Firma Microsoft, welches der Benutzerin oder dem Benutzer die Möglichkeit bietet, auf ein IT-System aus der Ferne zuzugreifen. Hierbei wird der komplette Bildschirminhalt übertragen, die Steuerung via Tastatur und Maus ist möglich und es werden noch weitere Services wie Druckfunktionalität zur Verfügung gestellt. Besonderes Augenmerk sollte man daher auf die Absicherung und Aktualisierung dieser Dienste legen.

Wie gravierend so eine Schwachstelle in einem kritischen System sein kann, zeigt der DoppelPaymer Ransomware-Angriff auf die Düsseldorfer Uniklinik. Wie im vierten Kapitel detailliert dargestellt, wurde dort eine Schwachstelle im Citrix Gateway (Shitrix) ausgenutzt.[142]

[142] Vgl. Citrix Systems. (2019). „CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance“.

Folgende Punkte sollten beim Absichern eines RDP Zugangs beachtet werden:[143]

- RDP Zugriff über ein VPN kapseln und nicht direkt im Internet anbieten
- Remote Desktop Gateway Server mit Zweifaktor-Authentifizierung verwenden
- IP-Adressbereich aus dem zugegriffen werden kann einschränken
- starke Passwörter verwenden
- RDP Standard Ports sollten geändert werden, um es Port Scannern zu erschweren
- Benutzerkreis möglichst einschränken

5.4.9 Beschränkung des Volume Shadow Copy Service (VSS)

Der Volume Shadow Copy Service ist ein von Microsoft entwickelter Dienst zur Erstellung von Schattenkopien, um der Anwenderin oder dem Anwender Zugriff auf verschiedene Versionsstände eigener Dateien zu ermöglichen. Dieser Dienst kann auch dazu verwendet werden, irrtümlich gelöschte oder beschädigte Dateien wiederherzustellen. Dies ist besonders nach einem erfolgreichen Ransomware-Angriff von Bedeutung.

Über den Befehl *„vssadmin.exe delete shadows /all /quiet“* ist es für Schadsoftware möglich, alle diese Schattenkopien zu löschen, ohne eine Meldung auszugeben.[144] Daher sollte der Zugriff auf diesen Befehl durch eine Gruppenrichtlinie blockiert werden.

5.4.10 Sperre von externen Schnittstellen

Gerade in großen Unternehmen oder Anlagen der kritischen Infrastruktur, die aus Sicherheitsgründen nicht direkt mit dem Internet verbunden sind, stellen externe Schnittstellen wie USB eine große Gefahr da. Daher sollten in diesen Bereichen die externen Schnittstellen von IT-Systemen bei Nichtverwendung immer gesperrt werden, um das Risiko durch infizierte USB-Sticks oder externe Festplatten zu minimieren.

5.4.11 Nutzersensibilisierung (User Awareness)

Wie die Analyse der Ransomware-Angriffe im vierten Kapitel gezeigt hat, sind die Benutzerinnen und Benutzer eine der größten Schwachstellen, wenn es um die erfolgreiche Infektion durch Ransomware geht. Der Stress und die Last im Alltag sowie Müdigkeit lassen selbst versierte Anwenderinnen und Anwender regelmäßig auf Phishing-Mails

[143] Vgl. Malwarebytes. (2020). „How to protect your RDP access from ransomware attacks“.
[144] Vgl. Microsoft. (2018). „vssadmin delete shadows“.

hereinfallen. Obendrein bedienen sich Kriminelle noch der menschlichen Psychologie und setzen auf die erfolgreiche Variante des CEO Fraud (Business Email Compromise), wobei der Mitarbeiterin oder dem Mitarbeiter in einem gefälschten E-Mail des Vorgesetzten vorgegaukelt wird, eine wichtige Datei sofort zu öffnen und bearbeiten zu müssen.

Erhält eine Anwenderin oder ein Anwender ein E-Mail mit verdächtigem Anhang, wie beispielsweise „BewerbungsmappePDF.exe“, sollte dieses sofort gelöscht werden, ohne den Inhalt zu öffnen. Des Weiteren sollten auch die in der Kontaktliste abgespeicherten Personen über des im Umlauf befindlichen E-Mails informiert werden, da nicht auszuschließen ist, dass sich dieses E-Mail anhand der Kontaktliste wurmartig verbreitet.

Phishing-Mails sind auch deshalb so unter Cyberkriminellen beliebt, weil diese über Bot-Netze kostengünstig in tausendfacher Kopie versendet werden können. Es gibt aber auch die besondere Variante des Spear-Phishings, bei der Organisationen und Personen gezielt angegriffen werden. Die umfangreiche Aus- und Weiterbildung der Benutzerinnen und Benutzer erweist sich als die wirksamste Möglichkeit gegen Phishing und Social Engineering im Allgemeinen.

KAPITEL 6

Rechtliche Aspekte von Ransomware-Angriffen

Die strafrechtliche Verfolgung von Ransomware-Angreiferinnen und Angreifern gestaltet sich äußerst schwierig. Um diese Ansprüche geltend zu machen, muss der Verursacher bekannt sein, was bei Ransomware-Angriffen selten der Fall sein dürfte, da diese durch zahlreiche Taktiken und Anonymisierungsdienste, wie das Onion Routing Netzwerk TOR, die Spuren ihres Angriffes erfolgreich verschleiern. Selbst wenn die Angreiferinnen oder Angreifer ausgeforscht werden können, ist es aufgrund fehlender internationaler Rechtshilfeabkommen nicht immer möglich, diese zur Verantwortung zu ziehen. Falls doch gestaltet sich dies oft als mühsamer und langwieriger Prozess, da etablierte Kommunikationswege und Hierarchien bei den Ermittlungen eingehalten werden müssen.

Wurde man erfolgreich durch eine Ransomware angegriffen, hat man grundsätzlich zwei Möglichkeiten. Entweder man stellt eine Strafanzeige und schließt sich dieser als Privatbeteiligter an oder man stellt den zivilrechtlichen Anspruch auf Schadenersatz, trägt hierbei aber das volle Prozessrisiko.

6.1 Österreichisches Strafrecht

Die folgenden Paragraphen des österreichischen Strafrechts können mitunter bei einem Ransomware-Angriff angewendet werden, wobei der Fokus auf Angriffen der kritischen Infrastruktur liegt. Hierbei muss allerdings immer der objektive und subjektive Tatbestand abgewogen werden. Die kritische Infrastruktur wird im Strafgesetzbuch wie folgt definiert:

§ 74 Abs. 1 Z 11 kritische Infrastruktur - *Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Landesverteidigung oder den Schutz der Zivilbevölkerung gegen Kriegsgefahren, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, das öffentliche Abfallentsorgungs- und Kanalwesen oder den öffentlichen Verkehr haben.*[145]

Der folgende Paragraph kann zur Anwendung kommen, falls bei dem Ransomware-Angriff Daten beschädigt oder zerstört werden, die einen gewissen Vermögenswert haben. Kein Schaden liegt hierbei allerdings vor, wenn die verschlüsselten Daten keinen Wert haben oder ohnehin zur Löschung vorgesehen waren.

§ 126a StGB Datenbeschädigung - *Wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Wird das Delikt gegen eine kritische Infrastruktur ausgeführt oder im Rahmen einer kriminellen Vereinigung, kann die Freiheitsstrafe bis zu fünf Jahre betragen.*[146]

Ob eine Erpressung gemäß § 144 StGB bei einem Ransomware-Angriff vorliegt, ist äußerst strittig, da der Paragraph in erster Linie auf die Anwendung physischer Gewalt abzielt. Es kann unter Umständen eine Drohung am Vermögen geltend gemacht werden, wenn die verschlüsselten Daten wertvoll sind, aber dies ist in jeder Strafsache individuell vom Gericht zu entscheiden und hängt auch von der Höhe des Lösegeldes ab.

[145] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF.“ § 74 Abs. 1 Z 11.

[146] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF.“ § 126a.

§ 144 StGB Erpressung - *Wer jemanden mit Gewalt oder durch gefährliche Drohung zu einer Handlung, Duldung oder Unterlassung nötigt, die diesen oder einen anderen am Vermögen schädigt, ist, wenn er mit dem Vorsatz gehandelt hat, durch das Verhalten des Genötigten sich oder einen Dritten unrechtmäßig zu bereichern, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.*[147]

Handelt es sich bei den Angreiferinnen und Angreifern um eine Gruppierung aus mehreren Personen, die über einen längeren Zeitraum besteht, dann kann auch der § 278 StGB angewendet werden.[148] Im Fall, dass dies gewerbsmäßig geschieht, wird nach § 145 Abs. 2 Z 1 StGB sogar schwerer Betrug schlagend.[149] Es ist zwar äußerst umstritten, kann aber unter Umständen auch für das Opfer weitreichende Folgen haben, denn wenn eine Zahlung des Lösegeldes erfolgen sollte, so steht gemäß § 278 Abs. 3 StGB die Finanzierung einer kriminellen Vereinigung im Raum.[150] Da die Zahlung des Lösegeldes allerdings rechtswidrig ist, könnte das Opfer gemäß § 10 StGB einen entschuldigenden Notstand geltend machen.[151,152,153]

§ 278 StGB Kriminelle Vereinigung - *Eine kriminelle Vereinigung ist ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern der Vereinigung ein oder mehrere Verbrechen, andere erhebliche Gewalttaten gegen Leib und Leben, nicht nur geringfügige Sachbeschädigungen, Diebstähle oder Betrügereien, Vergehen nach den §§ 165, 177b, 233 bis 239, 241a bis 241c, 241e, 241f, 283, 304 oder 307, in § 278d Abs. 1 genannte andere Vergehen oder Vergehen nach den §§ 114 Abs. 1 oder 116 des Fremdenpolizeigesetzes ausgeführt werden.*[154]

Je nachdem wie die Ransomware auf das zu verschlüsselnde Zielsystem gelangt, können auch noch weitere Paragraphen im Strafrecht schlagend werden. Der folgende Paragraph

[147] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 144.
[148] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 278.
[149] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 145 Abs. 2 Z 1.
[150] Plöchl. (2018). „Höpfel/Ratz, WK StGB, 2. Auflage", Rz 38 und 46.
[151] Plöchl. (2018). „Höpfel/Ratz, WK StGB, 2. Auflage", Rz 46.
[152] Fuchs. (2018). *Strafrecht Allgemeiner Teil I - Grundlagen und Lehre von der Straftat*, S. 245 ff.
[153] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 10.
[154] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 278.

kann zur Anwendung gelangen, wenn beispielsweise Passwörter gehackt werden, um sich Zugang zu einem System zu verschaffen. Die Ausnützung von Schwachstellen wie EternalBlue fällt allerdings nicht darunter, da hier keine Sperren umgangen werden. Die Angreiferin oder der Angreifer wird auch nur mit Ermächtigung des Opfers verfolgt, wovon viele Firmen aus Reputationsgründen allerdings absehen.

§ 118a StGB Widerrechtlicher Zugriff auf ein Computersystem - *Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*[155]

6.2 Zivilrechtlicher Schadenersatz

Doch nicht nur die strafrechtliche Verfolgung der Täterinnen und Täter gestaltet sich als komplexes Szenario. Der amerikanische Lebensmittelkonzern Mondolez, zu dem auch Marken wie Toblerone gehören, hat den Schweizer Versicherungskonzern Zurich verklagt, weil dieser nach dem erfolgreichen Not-Petya Angriff keinen Schadensersatz in Millionenhöhe zahlen wollte, da es sich bei den Angreifern um staatliche Akteure gehandelt hat und der Angriff als Krieg eingestuft wurde.[156] Ähnlich gestaltet sich der Fall des Pharmakonzernes Merck Sharp und Dohme.

6.3 EU-Sanktionen und internationales Recht

Die Anwendung des Rechts gestaltet sich noch wesentlich komplexer, falls es sich bei den Angreiferinnen und Angreifern um staatliche Akteure handelt. Dies war offensichtlich bei der WannaCry und Not-Petya, sowie der Angriffswelle auf den Deutschen Bundestag der Fall. Hinter dem WannaCry Angriff dürfte die Nordkoreanische Volksrepublik stehen, die im Westen Chaos stiften und die Erlöse der Erpressungen zur Finanzierung ihres

[155] Republik Österreich. (1974). „Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF." § 118a.

[156] Vgl. The NY Times. (2019). „Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong."

Atomprogrammes verwendete. Hinter der Not-Petya Angriffswelle, sowie dem Deutschen Bundestag wird Russland vermutet. Deshalb hat die EU im Oktober 2020 ihre Sanktionen gegen Russland ausgeweitet.[157] Die US-Regierung geht hingegen gegen nordkoreanische Hacker vor.[158]

[157]Vgl. Europäische Union. (2020). „Beschluss (GASP) 2020/1537 des Rates vom 22. Oktober 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen“.

[158]Vgl. United States District Court. (2018). „Criminal Complaint MJ18-1479“.

KAPITEL 7

Fazit und Ausblick

Cyberangriffe auf Basis von Ransomware sind keine gänzlich neuartige Erfindung. Die grundlegenden Konzepte dieser Erpressungsvariante traten schon Ende der 1980er Jahre beim AIDS Trojan auf.[159] Vor allem aber in Hinblick auf die Anzahl der geschädigten oder gar zerstörten IT-Systeme, sowie den Summen der erpressten Lösegelder in Millionenhöhe, stellen die Angriffe der letzten Zeit eine neue Dimension dar. Zahlreiche Angriffe mittels der Ryuk Ransomware bei denen über 61 Millionen US-Dollar Lösegeld erpresst wurde, sowie der verheerende aus der Ukraine ausgehende Not-Petya Ransomware-Angriff im Jahre 2017 haben dies gezeigt.[160]

In den Anfängen waren vor allem Windows-Privatbenutzerinnen und Privatbenutzer Ziel von Ransomware-Angriffen, da diese oftmals technisch weniger versiert sind und weniger Schutzmaßnahmen auf deren IT-Systemen installiert haben. Allerdings konnten von privaten Personen nur geringe Lösegelder erpresst werden, weshalb sich Cyberkriminelle zunehmend auf finanzkräftige Unternehmen und Einrichtungen der kritischen Infrastruktur konzentrieren. Denn wie die Analyse der zahlreichen Angriffe im dritten und vierten Kapitel gezeigt hat, haben hinsichtlich des Angriffsvektors alle Bereiche dasselbe Problem. Schlecht gewartete IT-Systeme, ohne aktuelle Sicherheitsaktualisierungen stellen nach wie vor ein großes Problem dar. Dies war besonders bei der EternalBlue Schwachstelle zu beobachten, wie lange es gedauert hat, bis potentiell angreifbare IT-Systeme die notwen-

[159] Vgl. Virus Bulletin. (1990). *AIDS Information Version 2.0*, S. 2.
[160] FBI. (2020). „Feds Fighting Ransomware: How the FBI Investigates and How You Can Help“, S. 23.

digen Patches erhalten haben.[161] Auch für Unternehmen, die Sicherheitsaktualisierungen üblicherweise einige Wochen zurückhalten, bis diese auf vollständige Kompatibilität geprüft wurden, hat dies enorme Auswirkungen. Des Weiteren gilt zu beachten, dass aktuelle Anti-Mailware Software zwar viele Schadprogramme erkennen, bei neueren ausgefeilten Ransomware-Angriffen oder Schwachstellen im System, wie beispielsweise die Remote Code Execution Schwachstelle im Windows SMB Protokoll der Version 1, keinerlei Schutz bieten.

Das zweite große Problem stellen fehlerhafte oder schlichtweg nicht vorhandene Datensicherungen dar, mit denen man den Schaden eines Ransomware-Angriffes in Grenzen halten kann. Gerade unter privaten Benutzerinnen und Benutzern sind regelmäßige Datensicherungen nach wie vor eine Seltenheit, obwohl es zahlreiche gute Lösungswege gibt. Aber auch bei Unternehmen werden zwar regelmäßig Datensicherungen erstellt, diese dann aber nie getestet und zurück eingespielt. Dies ist gerade bei Ransomware-Varianten, die sofort nach Infektion mit der Verschlüsselung beginnen, besonders verheerend. Denn oft werden dann die verschlüsselten Daten gesichert und überschreiben somit funktionierende Datensicherungen, falls der Ransomware-Angriff nicht sofort erkannt wird.

Das größte Problem hinsichtlich der Ransomware-Angriffe zeigt sich jedoch auf Ebene der Anwenderinnen und Anwender. Die mangelnde Kenntnis, Ausbildung und Sensibilisierung für diese Art von Cyberangriffen sind besonders gravierend. Gerade Phishing-Mails mit infizierten Anhängen oder Links zu Schadcode gehören zu den häufigsten und effektivsten Angriffsvektoren.[162] Daher ist es gerade für Unternehmen und Betreiber von kritischer Infrastruktur besonders wichtig, hier entsprechende Maßnahmen zu setzen und die Mitarbeiterinnen und Mitarbeiter regelmäßig auf dem neusten technischen Stand der Dinge zu halten und für potentielle Angriffsvarianten zu sensibilisieren.

Zweifellos hat auch das Aufkommen der Kryptowährungen, insbesondere die weite Verbreitung von Bitcoin, dazu beigetragen, dass Ransomware-Angriffe bei Kriminellen immer beliebter werden.[163] Waren früher aufwendige Konstruktionen mit Hilfe von Verrechnungsschecks und Postfächer sowie Nummernkonten in Panama oder anderen exotischen Ländern notwendig, erleichtern die weitgehend anonymen Transaktionen der Kryptowährungen die Erpressungen mit Lösegeldern enorm. Dabei wird auch, wie im zweiten Kapitel

[161] Vgl. Microsoft Security Bulletin. (2017). „MS17-010 - Critical“.
[162] Vgl. Gallegos et al. (2017). „Social engineering as an attack vector for ransomware“.
[163] Vgl. Kshetri und Voas. (2017). „Do Crypto-Currencies Fuel Ransomware?“, S. 11.

erläutert, auf Techniken wie beispielsweise einem Bitcoin-Mixer zurückgegriffen, um die Transaktionen der erpressten Lösegelder wie bei der klassischen Geldwäsche zu verschleiern.[164] Die Abbildung 7.1 zeigt deutlich, wie monetär lukrativ die Ransomware-Angriffe für Kriminelle in den letzten Jahren waren.

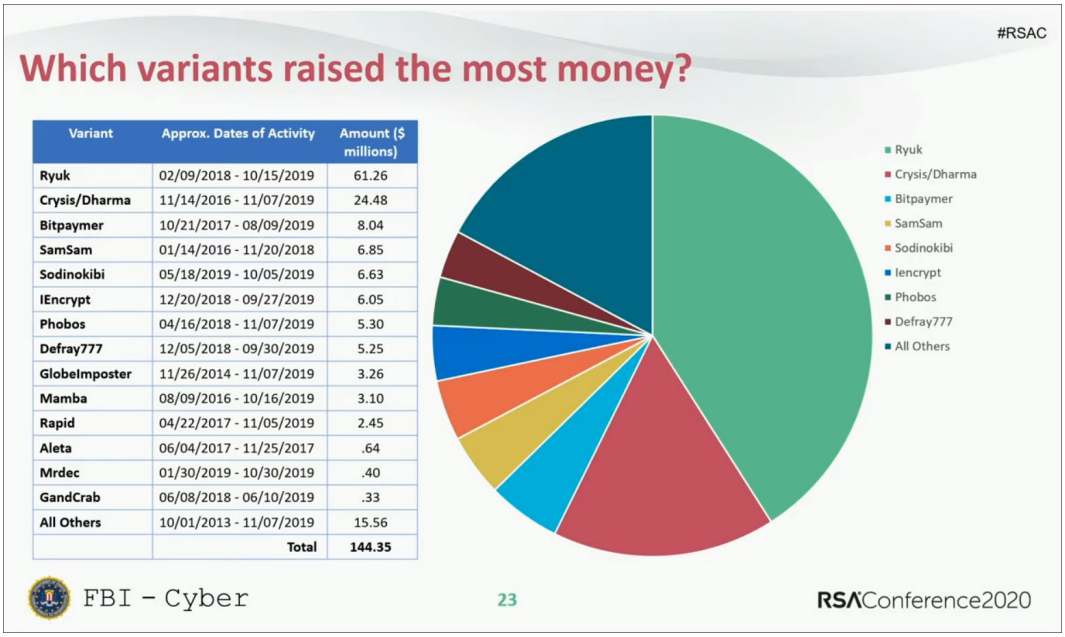

Abbildung 7.1: Aufschlüsselung der erpressten Lösegelder nach Ransomware[165]

Auch die zunehmende Verwendung und Integration von Internet of Things (IoT) Geräten in unserem Alltag schafft einen großen Angriffsvektor.[166] Viele der derzeit angebotenen Geräte, vor allem für die Heimautomatisierung, bieten keinen oder nur einen äußerst unzureichenden Schutz. Etliche Internet of Things Geräte können nur schlecht anders konfiguriert werden oder erhalten nach Erscheinen keine weiteren Sicherheitsaktualisierungen vom Hersteller mehr. Zwei EU-Richtlinien über vertragsrechtliche Aspekte digitaler Inhalte und digitaler Dienstleistungen (DIRL, Richtlinie (EU) 2019/770) und weiters die Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs (WKRL, Richtlinie

[164] Vgl. Bundeskriminalamt. (2019). *Cybercrime Report 2019*, S. 20.
[165] FBI. (2020). „Feds Fighting Ransomware: How the FBI Investigates and How You Can Help“, S. 23.
[166] Vgl. Yaqoob et al. (2017). „The rise of ransomware and emerging security challenges in the Internet of Things“, S. 1–15.

(EU) 2019/771) wurden dahingehend auf den Weg gebracht und sind im Laufe dieses Jahres 2021 in österreichisches Recht umzusetzen.[167,168]

Ein weiteres Phänomen zeigten vor allem auch die Angriffe mit Hilfe der GandCrab Ransomware, die auf Basis von Ransomware as a Service (RaaS) angeboten wird.[169] Wie im zweiten Kapitel erläutert, werden bei Ransomware as a Service die Angriffe nicht von den Kriminellen selbst durchgeführt, sondern die Werkzeuge, wie die für den Angriff benötigte Schadsoftware, anderen Angreiferinnen und Angreifern zur Verfügung gestellt. Angeboten werden diese Dienstleistungen vorwiegend im Darknet und das zu relativ erschwinglichen Preisen beziehungsweise werden die Entwickler der Schadsoftware an den erpressten Lösegeldern beteiligt. Somit sind auch technisch weniger versierte Kriminelle in der Lage, hoch komplexe Angriffe zu starten. Dies zeigt sich auch gerade in Zeiten der COVID-19 Pandemie, in der aufgrund der zahlreichen Ausgangssperren und des Home-Offices die Hauseinbrüche gesunken sind und viele Kriminelle auf andere Einkommensquellen umsteigen mussten. Aus all diesen Gründen werden Ransomware-Angriffe noch lange an der Tagesordnung stehen, sowohl im privaten Bereich, als auch bei großen Unternehmen und Einrichtungen der kritischen Infrastruktur.

[167] Vgl. Europäische Union. (2019). „Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen“.

[168] Vgl. Europäische Union. (2019). „Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG“.

[169] Vgl. Bundeskriminalamt. (2019). *Cybercrime Report 2019*, S. 19.

Literatur

Bücher

Fuchs, H. (2018). *Strafrecht Allgemeiner Teil I - Grundlagen und Lehre von der Straftat*.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*.

Liska, A. & Gallo, T. (2016). *Ransomware: Defending Against Digital Extortion*. O'Reilly Media, Inc.

Artikel

Aalborg, H. A., Molnár, P. & de Vries, J. E. (2019). What can explain the price, volatility and trading volume of Bitcoin? *Finance Research Letters*, *29*, 255–265. https://doi.org/https://doi.org/10.1016/j.frl.2018.08.010

Adamov, A. & Carlsson, A. (2017). The state of ransomware. Trends and mitigation techniques, 1–8. https://doi.org/10.1109/EWDTS.2017.8110056

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/https://doi.org/10.1016/S1353-4858(16)30086-1

Chakraborty, S. (2017). A Comparison study of Computer Virus and Detection Techniques. *Research Journal of Engineering and Technology*, *8*(1), 49. https://doi.org/10.5958/2321-581x.2017.00008.3

Gallegos, P., Bravo-Torres, J., Larios-Rosillo, V., Vintimilla Tapia, P., Yuquilima, I. & Jara, J. (2017). Social engineering as an attack vector for ransomware, 1–6. https://doi.org/10.1109/CHILECON.2017.8229528

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine*, *2*(1), 98. https://doi.org/10.1038/s41746-019-0161-6

Kshetri, N. & Voas, J. (2017). Do Crypto-Currencies Fuel Ransomware? *IT Professional*, *19*, 11–15. https://doi.org/10.1109/MITP.2017.3680961

Plöchl, F. (2018). Höpfel/Ratz, WK StGB, 2. Auflage. Zugriff am 30. Jänner 2021 unter https://rdb.manz.at/document/1141_18_stgb_p0278

TK, A. (2017). Discussion On Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks. *International Journal of Science and Engineering Development Research (www.ijrti.org)*, *2*, 310–314. Zugriff am 15. Dezember 2020 unter https://www.ijrti.org/papers/IJRTI1706057.pdf

Vujičić, D., Jagodić, D. & Ranđić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview, 1–6. https://doi.org/10.1109/INFOTEH.2018.8345547

Weckstén, M., Frick, J., Sjöström, A. & Järpe, E. (2016). A novel method for recovery from Crypto Ransomware infections, 1354–1358. https://doi.org/10.1109/CompComm.2016.7924925

Yaqoob, I., Ahmed, E., Habib ur Rehman, M., Ahmed, A. I. A., Al-Garadi, M., Imran, M. & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*. https://doi.org/10.1016/j.comnet.2017.09.003

Young, A. & Moti Yung. (1996). Cryptovirology: extortion-based security threats and countermeasures, 129–140. https://doi.org/10.1109/SECPRI.1996.502676

Yuan, Y. & Wang, F. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1421–1428. https://doi.org/10.1109/TSMC.2018.2854904

Technische Berichte

Bitdefender. (2016). *Petya Ransomware Goes Low Level* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://download.bitdefender.com/resources/files/News/file/Bitdefender-2016-Windows_Ransomware_Goes_Low_Level-Petya-Whitepaper.pdf

Bundeskriminalamt. (2019). *Cybercrime Report 2019* (Techn. Ber.). Zugriff am 15. Jänner 2021 unter https://bundeskriminalamt.at/306/files/Cybercrime_2019.pdf

Kaspersky. (2020). *Ransomware Revealed: Paying for the Protection of your Privacy* (Techn. Ber.).

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS* (Techn. Ber.). Zugriff am 15. Jänner 2021 unter https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf

SophosLabs. (2013). *Ransomware: Next-Generation Fake Antivirus* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/SophosRansomwareFakeAntivirus.pdf

SophosLabs. (2019). *WannaCry Aftershock* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf

Symantec. (2016a). *Internet Security Threat Report* (Techn. Ber.). Zugriff am 10. Dezember 2020 unter https://docs.broadcom.com/doc/istr-21-2016-en

Symantec. (2016b). *Ransomware and Business, ISTR Special Report* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5c_ISTR2016_Ransomware_and_Businesses.pdf

The Computer Emergency Response Team of Mauritius. (2017). *The Petya Cyber Attack* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter http://cert-mu.govmu.org/English/Documents/White%20Papers/PETYA%20CYBER%20ATTACK%20-%20CERTMU%20WHITEPAPER.pdf

Virus Bulletin. (1990). *AIDS Information Version 2.0* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

Virus Bulletin. (1992). *Popp Goes The Weasel* (Techn. Ber.). Zugriff am 15. Dezember 2020 unter https://www.virusbulletin.com/uploads/pdf/magazine/1992/199201.pdf

Onlinequellen

BBC. (2019, 7. August). *North Korea stole 2bn USD for weapons via cyber-attacks.* Zugriff am 15. Jänner 2021 unter https://www.bbc.com/news/world-asia-49259302

BleepingComputer. (2020, 28. September). *UHS hospitals hit by reported country-wide Ryuk ransomware attack.* Zugriff am 15. Jänner 2021 unter https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

Bloomberg. (2020, 28. Jänner). *Ransomware Linked to Iran, Targets Industrial Controls.* Zugriff am 15. Jänner 2021 unter https://www.bloomberg.com/news/articles/2020-01-28/-snake-ransomware-linked-to-iran-targets-industrial-controls

Check Point Research. (2017, 29. September). *EternalBlue – Everything There Is To Know.* Zugriff am 15. Jänner 2021 unter https://research.checkpoint.com/2017/eternalblue-everything-know/

Citrix Systems. (2019, 17. Dezember). *CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance.* Zugriff am 15. Jänner 2021 unter https://support.citrix.com/article/CTX267027

CNBC. (2017). *Petya ransomware: All you need to know about the cyberattack and how to tell if you're at risk.* Zugriff am 15. Dezember 2020 unter https://www.cnbc.com/2017/06/28/petya-ransomware-cyberattack-explained-how-to-tell-if-youre-at-risk-or-been-attacked.html

Cyble. (2020, 20. Mai). *NetWalker Ransomware Operators Targets City of Weiz – Data Leak.* Zugriff am 15. Dezember 2020 unter https://cybleinc.com/2020/05/20/netwalker-ransomware-operators-targets-city-of-weiz-data-leak/

DerStandard. (2020, 24. Mai). *Hacker sollen interne Daten der steirischen Stadt Weiz veröffentlicht haben.* Zugriff am 15. Dezember 2020 unter https://www.derstandard.at/story/2000117665649/bericht-hacker-veroeffentlichen-interne-daten-der-steirischen-stadt-weiz

Deutsche Bahn AG. (2019). *Kennzahlen.* Zugriff am 15. Dezember 2020 unter https://www.deutschebahn.com/de/konzern/konzernprofil/zahlen_fakten/kennzahlen_2019-5058430

Dragos. (2020, 2. März). *EKANS Ransomware and ICS Operations*. Zugriff am 15. Jänner 2021 unter https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

ESET. (2017, 24. Oktober). *Kiev metro hit with a new variant of the infamous Diskcoder ransomware*. Zugriff am 15. Jänner 2021 unter https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/

Europol European Cybercrime Centre. (2016). *Crypto Sheriff*. Zugriff am 15. Jänner 2021 unter https://www.nomoreransom.org/crypto-sheriff.php

FBI. (2020). *Feds Fighting Ransomware: How the FBI Investigates and How You Can Help*. Zugriff am 15. Jänner 2021 unter https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17627/2020_USA20_SEM-M03H_01_Feds-Fighting-Ransomware-How-the-FBI-Investigates-and-How-You-Can-Help.pdf

Fire Eye. (2017, 23. Mai). *WannaCry Malware Profile*. Zugriff am 15. Dezember 2020 unter https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

FortiGuard Labs. (2020, 5. März). *Ryuk Revisited - Analysis of Recent Ryuk Attack*. Zugriff am 15. Jänner 2021 unter https://www.fortinet.com/blog/threat-research/ryuk-revisited-analysis-of-recent-ryuk-attack

Heise. (2017, 13. Mai). *Ransomware WannaCry befällt Rechner der Deutschen Bahn*. Zugriff am 15. Dezember 2020 unter https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html

Heise. (2020a, 17. September). *Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau*. Zugriff am 15. Dezember 2020 unter https://www.heise.de/news/Hackerangriff-auf-Uniklinik-Duesseldorf-Ermittlungen-wegen-fahrlaessiger-Toetung-4904134.html

Heise. (2020b, 22. September). *Uniklinik Düsseldorf: Ransomware DoppelPaymer soll hinter dem Angriff stecken*. Zugriff am 15. Dezember 2020 unter https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html

Independent. (2017, 27. Juni). *Petya cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack*. Zugriff am 15. Jänner 2021 unter https://www.

independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

Internet Engineering Task Force. (1999). *Anti-Spam Recommendations for SMTP MTAs*. Zugriff am 30. Jänner 2021 unter https://tools.ietf.org/html/rfc2505

Interpol. (2020, 4. April). *Cybercriminals targeting critical healthcare institutions with ransomware*. Zugriff am 15. Dezember 2020 unter https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Kaspersky Lab Securelist. (2017a, 24. Oktober). *Bad Rabbit ransomware*. Zugriff am 15. Jänner 2021 unter https://securelist.com/bad-rabbit-ransomware/82851/

Kaspersky Lab Securelist. (2017b, 28. Juni). *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*. Zugriff am 15. Dezember 2020 unter https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Kaspersky Lab Securelist. (2017c, 27. Juni). *Schroedingers Pet(ya)*. Zugriff am 15. Dezember 2020 unter https://securelist.com/schroedingers-petya/78870/

Malwarebytes. (2016, 1. April). *Petya – Taking Ransomware To The Low Level*. Zugriff am 15. Dezember 2020 unter https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

Malwarebytes. (2017, 24. Juli). *Bye, bye Petya! Decryptor for old versions released*. Zugriff am 15. Dezember 2020 unter https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/

Malwarebytes. (2020a, 22. Februar). *How to protect your RDP access from ransomware attacks*. Zugriff am 15. Jänner 2021 unter https://blog.malwarebytes.com/security-world/business-security-world/2018/08/protect-rdp-access-ransomware-attacks/

Malwarebytes. (2020b). *Ryuk ransomware*. Zugriff am 15. Jänner 2021 unter https://www.malwarebytes.com/ryuk-ransomware/

McAfee Knowledge Center. (2020, 5. Oktober). *Protecting against modified Petya and BadRabbit ransomware variants*. Zugriff am 15. Dezember 2020 unter https://kc.mcafee.com/corporate/index?page=content&id=KB89540

Microsoft. (1998, 12. Oktober). *Microsoft Outlook 2000 Joins Office 2000 Suite in Supporting Visual Basic for Applications*. Zugriff am 30. Jänner 2021 unter

https://news.microsoft.com/1998/10/12/microsoft-outlook-2000-joins-office-2000-suite-in-supporting-visual-basic-for-applications/

Microsoft. (2009). *Volume shadow copy overview*. Zugriff am 15. Jänner 2021 unter https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc784351(v=ws.10)

Microsoft. (2018, 18. Mai). *vssadmin delete shadows*. Zugriff am 15. Jänner 2021 unter https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin-delete-shadows

Microsoft. (2020). *PowerShell Security Set-ExecutionPolicy*. Zugriff am 15. Jänner 2021 unter https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.1

Microsoft Security. (2016, 22. März). *New feature in Office 2016 can block macros and help prevent infection*. Zugriff am 15. Jänner 2021 unter https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Microsoft Security Bulletin. (2017, 14. März). *MS17-010 - Critical*. Zugriff am 15. Dezember 2020 unter https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft Security Response Center. (2017, 12. Mai). *Customer Guidance for WannaCrypt attacks*. Zugriff am 15. Dezember 2020 unter https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Microsoft Tech Community. (2019, 4. Oktober). *SMB1 Product Clearinghouse*. Zugriff am 15. Jänner 2021 unter https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb1-product-clearinghouse/ba-p/426008

Posteo. (2017, 27. Juni). *Info on the PetrWrap/Petya ransomware: Email account in question already blocked since midday*. Zugriff am 30. Jänner 2021 unter https://posteo.de/en/blog/info-on-the-petrwrappetya-ransomware-email-account-in-question-already-blocked-since-midday

Stadtgemeinde Weiz. (2020, 1. Oktober). *Stadtinformation und Geschichte*. Zugriff am 15. Dezember 2020 unter https://www.weiz.at/Gemeinde/Stadtinformation_Geschichte/Stadtinformation

The Guardian. (2017, 27. Juni). *Petya ransomware attack: what is it and how can it be stopped?* Zugriff am 15. Dezember 2020 unter https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

The NY Times. (2017, 12. November). *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*. Zugriff am 15. Dezember 2020 unter https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

The NY Times. (2019, 15. April). *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.* Zugriff am 15. Jänner 2021 unter https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

The Register. (2017, 28. Juni). *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide*. Zugriff am 15. Dezember 2020 unter https://www.theregister.com/2017/06/28/petya_notpetya_ransomware/

The Telegraph. (2017, 13. Mai). *Cyber attack hits German train stations as hackers target Deutsche Bahn*. Zugriff am 15. Dezember 2020 unter https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/

The Verge. (2017, 3. Juli). *Ukranian company that spread Petya could face criminal charges for vulnerability*. Zugriff am 15. Dezember 2020 unter https://www.theverge.com/2017/7/3/15916060/petya-medoc-vulnerability-ransomware-cyberattack

Trend Micro. (2020a, 18. Mai). *Reflective Loading Runs Netwalker Fileless Ransomware*. Zugriff am 15. Dezember 2020 unter https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

Trend Micro. (2020b, 15. Mai). *Threat Encyclopedia Ransom.PS1.NETWALKER.B*. Zugriff am 15. Dezember 2020 unter https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.PS1.NETWALKER.B?_ga=2.193533613.1079877318.1590136763-1671730187.1589220654

United States District Court. (2018). *Criminal Complaint MJ18-1479*. Zugriff am 15. Jänner 2021 unter https://www.justice.gov/opa/press-release/file/1092091/download

Universitätsklinikum Düsseldorf. (2017). *Geschäftsbericht*. Zugriff am 15. Dezember 2020 unter https://www.uniklinik-duesseldorf.de/fileadmin/Presse/GB_2017_klein.pdf

Universitätsklinikum Düsseldorf. (2020, 18. September). *IT-Ausfall an der Uniklinik Düsseldorf*. Zugriff am 15. Dezember 2020 unter https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-189-it-ausfall-an-der-uniklinik-duesseldorf

US-CERT. (2017). *Alert (TA17-181A) Petya Ransomware*. Zugriff am 15. Dezember 2020 unter https://us-cert.cisa.gov/ncas/alerts/TA17-181A

VMware. (2020, 12. Februar). *VMware Carbon Black TAU: Ryuk Ransomware Technical Analysis*. Zugriff am 15. Jänner 2021 unter https://www.carbonblack.com/blog/vmware-carbon-black-tau-ryuk-ransomware-technical-analysis/

Wired. (2020, 11. November). *The untold story of a cyberattack, a hospital and a dying woman*. Zugriff am 15. Jänner 2021 unter https://www.wired.co.uk/article/ransomware-hospital-death-germany

World Health Organization. (2005, 5. September). *Chernobyl: the true scale of the accident*. Zugriff am 15. Jänner 2021 unter https://www.who.int/news/item/05-09-2005-chernobyl-the-true-scale-of-the-accident

Gesetze und Richtlinien

Europäische Union. (2019a). Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Zugriff am 15. Jänner 2021 unter http://data.europa.eu/eli/dir/2019/770/oj

Europäische Union. (2019b). Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG. Zugriff am 15. Jänner 2021 unter http://data.europa.eu/eli/dir/2019/771/oj

Europäische Union. (2020). Beschluss (GASP) 2020/1537 des Rates vom 22. Oktober 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen

gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen. Zugriff am 15. Jänner 2021 unter https://eur-lex.europa.eu/eli/dec/2020/1537/oj

Republik Österreich. (1974). Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) idgF. Zugriff am 15. Jänner 2021 unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296

UK Public General Acts. (1990). Computer Misuse Act. Zugriff am 15. Dezember 2020 unter https://www.legislation.gov.uk/ukpga/1990/18/contents

Abbildungsverzeichnis